SecurityAnnual

2021 EDITION

MARKET OUTLOOK AND INDUSTRY INSIGHTS

PUBLISHED BY TAG CYBER

- **LEAD AUTHORS –** Ed Amoroso, Katie Teitler
- **RESEARCH AND CONTENT –** David Hechler, Shawn Hopkins, Liam Baglivo, Stan Quintana, Andy McCool, Jennifer Bayuk, Matt Amoroso
- **MEDIA AND DESIGN –** Miles McDonald, Lester Goodman, Rich Powell

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871

September 17, 2020

TO THE READER:

WELCOME TO THE NEW 2021 EDITION OF THE SECURITY ANNUAL FROM TAG CYBER.

As the security community staggers into 2021, our mission is clear: With the world's attention focused on the challenges of racial bias, political tensions, and a stubborn pandemic, cyber threats *must not* be allowed to join the litany of serious issues facing our globe. Our collective objective must be to prevent this from occurring, and it's not just that we have insufficient capacity to handle *yet another* problem. Rather, cyber threats could produce large-scale disruption on par with our other global challenges.

We hate to introduce our annual security volume with such a stark, perhaps even depressing, message, but our approach at TAG Cyber has been to call things as we see them. And right now, we see storm clouds on the horizon. But like all weather patterns, it is not ordained that massively coordinated cyber threats to critical infrastructure will become the *Next Big Thing*. Rather, it is possible that we can change the trajectory. Hopefully, this volume will help in that regard.

For the past five years, we at TAG Cyber have published our Security Annual in the hopes that we might democratize insights into the technology, trends, and complexities of the cyber security industry. Unlike the pay-for-play nonsense we see from many of the larger so-called research and advisory companies with their billions in revenue, we seek to inform readers in an honest and unbiased manner on the best methods and techniques for cyber defense.

And while, unlike the big advisory firms, we might not have the balance sheet of a small nation, we do have our moments of joy – usually when we help someone reduce risk. Here's a snippet from the CISO of a power company: "Your research pointed us to several new areas of protection," he wrote in an email, "and after adjusting our enterprise security architecture, we stopped a couple of things that could have been bad."

That is why we do what we do.

Continued

Unlike in previous years where this annual was rigidly structured around our fifty TAG Cyber security controls (and they are now up to fifty-four controls, by the way – sorry), we chose to make this year's annual more like a magazine. The interviews with luminaries are still here, but we chose to make the book something you might actually like to bring to the beach. (And yes, we give you permission to nerd out on the beach. We certainly do.)

The articles include some of the better pieces we created during 2020 in our day-to-day writing, but also many newly commissioned articles that offer our perspectives on the industry. As always, we do not lower our standards for the uninitiated. If you do not understand the basics of cyber security, then you'll need to do some separate calisthenics to catch up. This book is not like those vapid Security Concepts for Dummies pamphlets on vendor tables at RSA.

That said, the book is also not written for the eleven people in the world who understand the mathematics of elliptic curve cryptography. Rather, it is developed and aimed at the working practitioner in the cyber security industry. This includes developers, managers, sales professionals, marketing experts, and yes – even board members (although Luddites are not welcome here. If you are clueless, then go grab a Gartner report.)

Many of you often ask about our growing team and our services at TAG Cyber, so while this is not a marketing brochure for our world-class, unique, lightweight, global, premise or cloud-resident, threat intelligence enabled, machine learning assisted, fully agentless, 100% passwordless, and quantum powered security solutions (*sigh*), I am happy to give you an update on how things have been going for us these past twelve months.

Apart from pausing the lease for our Manhattan digs until we have more clarity around COVID-19, we've rolled out many new services, primarily for enterprise customers. Our research subscription business is growing faster than we can keep up with, and we now deliver a student assisted security portal to many small- and medium-sized business. Nothing makes us happier than providing useful information to security teams, so we are a smiling camp these days.

As for all of you working in cyber defense, we sense a continued uneasiness and uncertainty around security. As we alluded in our introductory points, the possibility seems greater than ever that nation-states will take full advantage of global unrest and infrastructure change to pounce on unsuspecting targets. Companies are weak when they are undergoing change and when they are distracted. The pandemic has produced both conditions everywhere.

So, while we continue to coach an upbeat message to our enterprise and government clients, and while we continue to be superbly impressed with so many great innovations in cyber security technology from commercial vendors, we also agree that optimism might be a bit premature. Instead, we recommend that while you read the essays, articles, and reports in this volume, you take serious and honest inventory of your probably insufficient posture.

Organizations in 2021 must adopt a serious and determined approach to their defensive activities. This is a time for cyber security teams, enterprise IT departments, and government security agencies to do their best work. Pandemics might slow down travel and commerce, but we assure you that they do not slow down cyber offense. If anything, they provide sufficient cover for a serious malicious advancement. Be confident, be vigilant, but also be careful.

We wish you well this coming year, and we look forward to 2021 being better than the twelve-month period we are about to push into the history books. If you can say anything positive about 2020, perhaps it's that by setting such a low bar, it raises the prospects that the coming year will be so much better. Let's make sure the cyber security community does its part to contribute to this welcome improvement.

Stay safe, healthy, and secure – and we hope you enjoy our 2021 TAG Cyber Security Annual.

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber
New York City, New York

Continued

Continued

OVERVIEW OF THE TAG CYBER CONTROLS FOR 2021

Each year, our expert analysts review and update a list of what we refer to as the TAG Cyber Controls. Including a total this year of fifty-four entries, our list is best interpreted as those areas in which a Chief Information Security Officer (CISO) must include some measure of focus in their enterprise security program. The TAG Cyber Controls can be viewed as our best answer to the following reasonable question that we hear almost every day from CISOs: *What elements should I include specifically in my enterprise program?*

We understand that many might choose to answer this question with the myriad existing security frameworks available. On one end of the spectrum, for example, we have the large and comprehensive NIST Cybersecurity Framework (CSF) and its attendant ample collage of detailed security requirements in NIST 800-53. At the other end of the spectrum, we have the smaller and more accessible Center for Internet Security (CIS) Controls, which boils things down to twenty functional recommendations to reduce enterprise risk.

These frameworks, and all those in between – including the Payment Card Industry (PCI) Data Security Standard (DSS), the Health Insurance Portability and Accountability Act (HIPAA), and others – play some role in helping enterprise teams develop the best protection program. Even the emerging privacy-oriented frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) include useful ideas that will help enterprise teams ensure proper coverage in their programs.

But the challenge for our TAG Cyber team has been our observation that none of these frameworks are sufficient for our industry research and analysis, and none seemed to match our collective practical experience running live security programs, managing enterprise protection teams, and coaching working CISOs across every sector imaginable. Instead, the frameworks always seem to have some miss in their coverage. What purely commercial CISO really, for example, depends on a System Security Plan (SSP) as demanded in NIST? I mean, *really?*

THE CONTROLS

So, we developed the fifty-four controls based on experience in the trenches. It includes expected areas such as firewall platforms and multi-factor authentication while also including rarely mentioned CISO strategies such as working with value-added solution providers and managed security service providers (MSSPs) and Managed Detection and Response (MDR) vendors. And, as you can see in Figure 1, the TAG Cyber Controls are presented in a way that allows visual inspection at a glance, which explains why many refer to it as the Periodic Table of Security.

Enterprise Controls	Network Controls	Endpoint Controls	Governance Controls	Data Controls	Service Controls
1 Deception-Based Security	10 Public Key Infrastructure	19 Anti-Malware Tools	28 Digital Risk Management	37 Data Privacy Platform	46 Research and Advisory Services
2 Intrusion Detection/Prevention	11 Cloud Security Solutions	20 Endpoint and EDR Security	29 Crowdsourced Security Testing	38 Content Security	47 Information Assurance
3 User Behavioral Analytics	12 DDOS Security	21 Hardware Security	30 Cyber Insurance	39 Secure File Sharing	48 MSSP and MDR Services
4 Data Leakage Protection	13 Email Security	22 ICS/IoT Security	31 Governance, Risk, Compliance (GRC)	40 Data Encryption	49 Large Security Consulting Firms
5 Firewall Platform	14 Infrastructure Security	23 SIEM Platform	32 Incident Response	41 Digital Forensics	50 Small Security Consulting Firms
6 Application Security	15 Network Monitoring	24 Mobile Security	33 Penetration Testing	42 Enterprise Asset Inventory	51 Security Staff Recruiting
7 Web Application Firewall	16 Network Access Control	25 Password/ Privilege Mgmt	34 Continuous Attack Simulation	43 DevOps Security	52 Security Training and Awareness
8 Web Fraud Prevention	17 Secure Access/ Zero Trust	26 Authentication Security	35 Identity and Access Management	44 Vulnerability Management	53 Advanced Security R&D Support
9 Web Security Gateway	18 Attack Surface Protection	27 Voice Security	36 Threat Intelligence	45 Threat Hunting Tools	54 Value-Added Solution Providers

Figure 1. TAG Cyber Controls for 2021

The six categories used to organize the fifty-four controls – namely, *enterprise, network, endpoint, governance, data*, and *service* – were created to help enterprise teams differentiate between the entries. Admittedly, the categorization is not perfect, and any expert perusing the structure will find one or two examples quickly that might not exactly match up with their listed category. We therefore don't make too big a deal of the categories, and just use them as a presentation device versus something more substantive.

CONTROL DETAILS

In the sections below, we provide a brief description of the controls. Enterprise customers of TAG Cyber are provided with much more detail on the framework through comprehensive market reports that include trend analysis and vendor mappings for each control. Customers also receive tailored guidance on how best to optimize an enterprise security portfolio with the most suitable commercial vendors in each of the fifty-four areas.

ENTERPRISE CONTROLS

1. DECEPTION-BASED SECURITY

Enterprise teams will benefit from the introduction of deceptive traps that can contain malware on endpoints and networks and that make use of virtualization to avoid cascade of ongoing breaches.

2. INTRUSION DETECTION/PREVENTION

Passive inspection from intrusion detection systems and active mitigation (usually source shunning) from intrusion prevention systems are standard elements of most current enterprise security programs.

3. USER BEHAVIORAL ANALYTICS
Behavioral observation and analysis can be used to uncover evidence that certain user or device activity is indicative of an enterprise security policy violation, perhaps due to a malware infection.

4. DATA LEAKAGE PROTECTION
Automation can be used effectively to detect and even block the leakage of sensitive data from endpoints, servers, or other systems connected to an enterprise network.

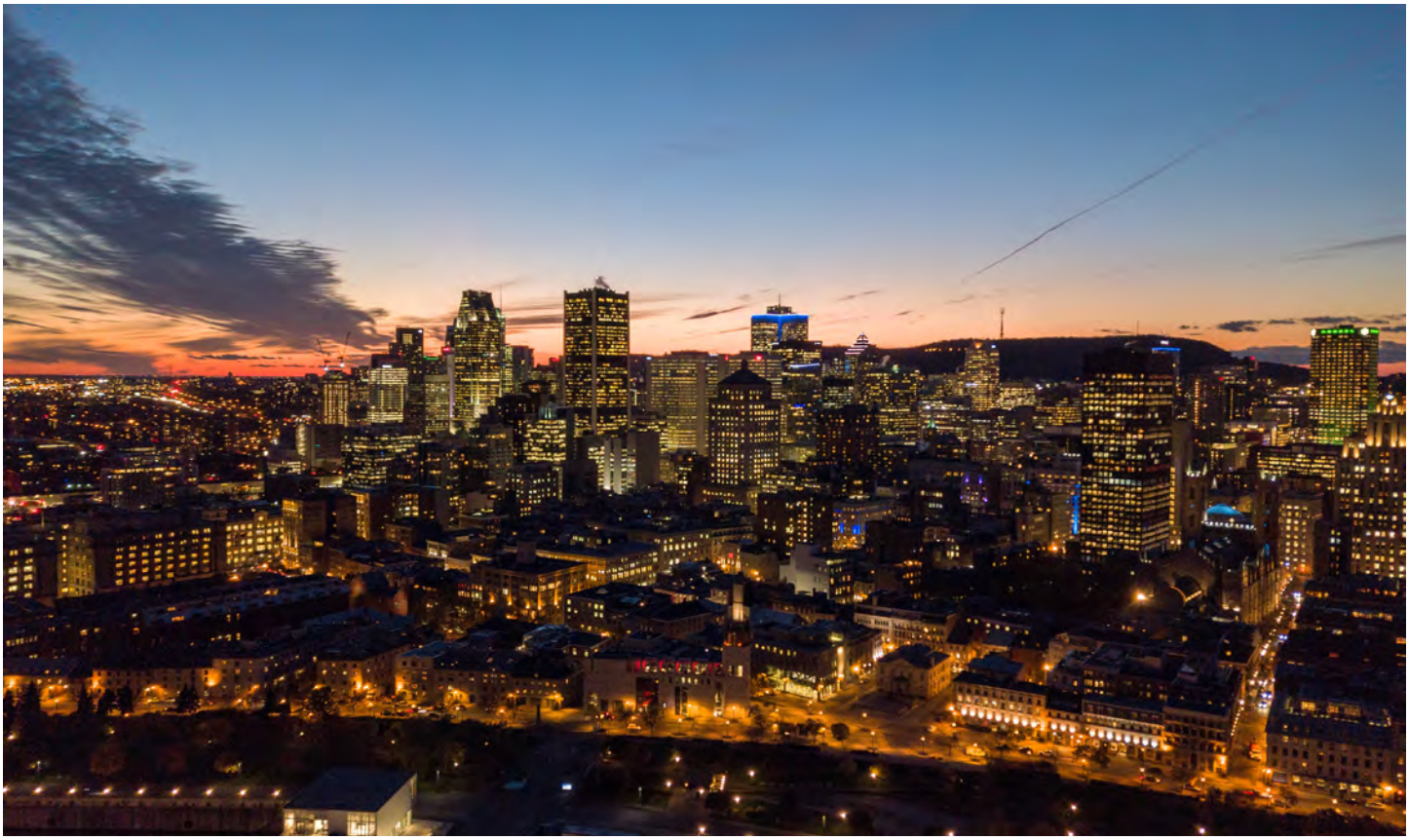
5. FIREWALL PLATFORM
Next-generation firewall platforms in an enterprise remain an essential aspect of the cyber security architecture, even in the face of de-perimeterization away from DMZs toward zero trust.

6. APPLICATION SECURITY
Most companies today would describe their business in terms of their suite of applications, which implies that application security becomes fundamental to protecting the organizational mission.

7. WEB APPLICATION FIREWALL
Enterprise security can be specifically tailored using web application firewalls (WAFs) that understand the details of how an application operates.

8. WEB FRAUD PREVENTION
Cyber security techniques for web fraud avoidance can be codified into devices that reside in the path of users and potential malicious actors accessing eCommerce applications.

9. WEB SECURITY GATEWAY
The web security gateway offers a safety net for enterprise teams hoping to avoid exfiltration of data from infected systems and offers policy enforcement for outbound browsing.



NETWORK CONTROLS

10. PUBLIC KEY INFRASTRUCTURE

Public key infrastructure (PKI)-based systems enable the deployment and use of public key technology for digital signatures and related cryptographic applications in the enterprise.

11. CLOUD SECURITY SOLUTIONS

Cloud-hosted applications, systems, and workloads require security controls to extend required policy enforcement beyond the enterprise premise and avoid cloud-specific cyber threats..

12. DDOS SECURITY

Botnet-originated denial of service threats continue to require security detection and mitigation, usually with network diversion to special off-line scrubbing firewalls, to ensure availability.

13. EMAIL SECURITY

The protection of email from phishing attacks and malware payloads has emerged in many enterprise contexts as the top cyber security risk – which helps explain the importance of email security tools.

14. INFRASTRUCTURE SECURITY

Addressing risks to the underlying infrastructure systems and protocols of the internet, such as the domain name system (DNS) and border gateway protocol (BGP) is an essential enterprise security task.

15. NETWORK MONITORING

Collecting, processing, and analyzing network traffic of all types via monitoring tools has always been an important component of every cyber security architecture.

16. NETWORK ACCESS CONTROL

The admission of devices to a local area network requires policy-based enforcement of access, which is typically done using a commercial network access control (NAC) system.

17. SECURE ACCESS/ZERO TRUST

The provision of access to cloud-hosted workloads without the protective cover of an enterprise perimeter is accomplished with secure access platforms implementing a zero trust security scheme.

18. ATTACK SURFACE PROTECTION

Enterprise security teams scan, collect, and analyze information about their entire visible surface, both inside and outside their perimeter, using commercial scanners and attack surface protection tools.

ENDPOINT CONTROLS

19. ANTI-MALWARE TOOLS

Software to detect and remove malware from PCs and other systems is one of the most mature and familiar aspects of both enterprise and personal cyber security.

20. ENDPOINT AND EDR SECURITY

The protection of endpoint systems from cyber threats is an essential task for an enterprise, and is increasingly focused on endpoint detection and response (EDR) services.

21. HARDWARE SECURITY
Protection of assets using hardware-based controls and capabilities has always been an important strategy, and continues to play an important role in modern enterprise.

22. ICS/IOT SECURITY
The emergence of industrial control system (ICS) and Internet of Things (IoT) as key considerations in enterprise cyber security is one of the more challenging areas of our industry.

23. SIEM PLATFORM
Most security architectures, especially for larger organizations, are centered on a SIEM-based collection and processing infrastructure with data connectors around the enterprise.

24. MOBILE SECURITY
Mobile infrastructure, systems, and devices require security controls to address their growing threat, especially as business and individuals continue to become more dependent on mobility.

25. PASSWORD/PRIVILEGE MANAGEMENT
The protection of passwords and privileges is essential, since the most critical enterprise administrative operations can be exploited using these authentication and authorization elements.

26. AUTHENTICATION SECURITY
The most basic primitive in cyber security involves the use of authentication solutions to validate reported identities by individuals, systems, workloads, and other entities.

27. VOICE SECURITY
Enterprise teams and individuals have tended to underestimate the risks associated with their use of voice, including mobile and the possibility of nation-state eavesdropping.

GOVERNANCE CONTROLS

28. DIGITAL RISK MANAGEMENT
The emergence of digital risk management protect brands through insights from web (deep, dark, and surface), social media, and other forums is an essential aspect of modern enterprise protection.

29. CROWDSOURCED SECURITY TESTING
The evolution of early bug bounties into modern crowdsourced security testing solutions has been an important risk reductive measure for most enterprise teams.

30. CYBER INSURANCE
The transfer of security risk from the enterprise to an insurance company has grown in popularity in recent years, especially with senior leadership teams and corporate boards.

31. GOVERNANCE, RISK, AND COMPLIANCE (GRC)
Governance, risk, and compliance tools provide a means for automated and continuous management of risk, including support for tasks such as gap analysis with targeted security frameworks.

32. INCIDENT RESPONSE
The response to security incidents is an essential task in enterprise, especially as more teams have come to recognize that serious attacks from capable actors cannot be prevented in most cases.

33. PENETRATION TESTING
Experts perform penetration tests against targeted enterprise systems to help demonstrate the existence of exploitable weaknesses before they might be detected by malicious actors.

34. CONTINUOUS ATTACK SIMULATION
The process of continuous attack simulation allows for demonstration that security controls are working properly, usually based on automated simulation of attacks using frameworks such as MITRE ATT&CK.

35. IDENTITY AND ACCESS MANAGEMENT
The day-to-day management of identities and coordination of access to applications, systems, and workloads via IAM systems is one of the more challenging aspects of modern enterprise cyber security.

36. THREAT INTELLIGENCE
Threat intelligence, whether manual or automated, provides essential data, information, context, and other views for enterprise cyber security teams dealing with day-to-day issues.

DATA CONTROLS

37. DATA PRIVACY PLATFORM
The emergence of stricter privacy protections and laws from various countries and states has introduced new platform obligations for anyone collecting and storing sensitive and personal information.

38. CONTENT SECURITY
The securing of content from fraud, unauthorized use, and other forms of abuse is a traditional aspect of how creative industries such as music protect their content.

39. SECURE FILE SHARING
Secure sharing of files between different individuals or groups is an essential protective component of any organization's collaboration environment.

40. DATA ENCRYPTION
The encryption of data is the most mature function in any enterprise security architecture, and remains a fundamental aspect of modern cyber protection of critical assets from unauthorized access.

41. DIGITAL FORENSICS
Investigators, including law enforcers, make use of digital forensic platforms to collect relevant evidence from devices as part of larger response and analysis activities.

42. ENTERPRISE ASSET INVENTORY
The performance of an enterprise asset inventory has shifted from a traditional IT-oriented activity to an important part of the underlying basis for cyber security protection.

43. DEVOPS SECURITY
Modern software teams must integrate security protections such as compliance evaluation and security testing into the DevOps process, thus resulting in a new process often referred to as DevSecOps.

44. VULNERABILITY MANAGEMENT
The management and analysis of existing and potential vulnerabilities in an enterprise is an important means for determining overall security risk and measuring accurate security posture.

45. THREAT HUNTING TOOLS
Threat analysts, often working in security operation center (SOC) environments, make use of modern threat hunting tools to optimize their ability to process and analyze data for response.

SERVICE CONTROLS

46. RESEARCH AND ADVISORY SERVICES

The research and advisory industry includes individuals who are expected to provide unbiased guidance on cyber security vendors to help enterprises optimize their portfolio programs.

47. INFORMATION ASSURANCE

The information assurance designation is used for enterprise security solution offerings that have been tailored to support the unique procurement, usage, and compliance needs of the federal government.

48. MSSP AND MDR SERVICES

Enterprise teams regularly use the services of a managed security service provider (MSSP) or managed detection and response (MDR) to complement in-house protection initiatives.

49. LARGE SECURITY CONSULTING FIRMS

Large security consulting firms can offer a more comprehensive range of professional service solutions for organizations with more complex threat and operational requirements.

50. SMALL SECURITY CONSULTING FIRMS

Small consulting firms can offer more tailored security support for specific requirements that might exist within organizations of all sizes and types.

51. SECURITY STAFF RECRUITING

The security staff recruiting function in an enterprise often benefits through partnership with a capable firm with contacts, insights, and experience in the cyber security industry.

52. SECURITY TRAINING AND AWARENESS

Ongoing awareness training of employees and specialized education of experts in security-related technology and methodologies are essential to the modern enterprise protection program.

53. ADVANCED SECURITY R&D SUPPORT

Research and development (R&D) support to address any special requirements or issues in a given organization or industry is essential to optimize threat prevention, detection, and response.

54. VALUE-ADDED SOLUTION PROVIDERS

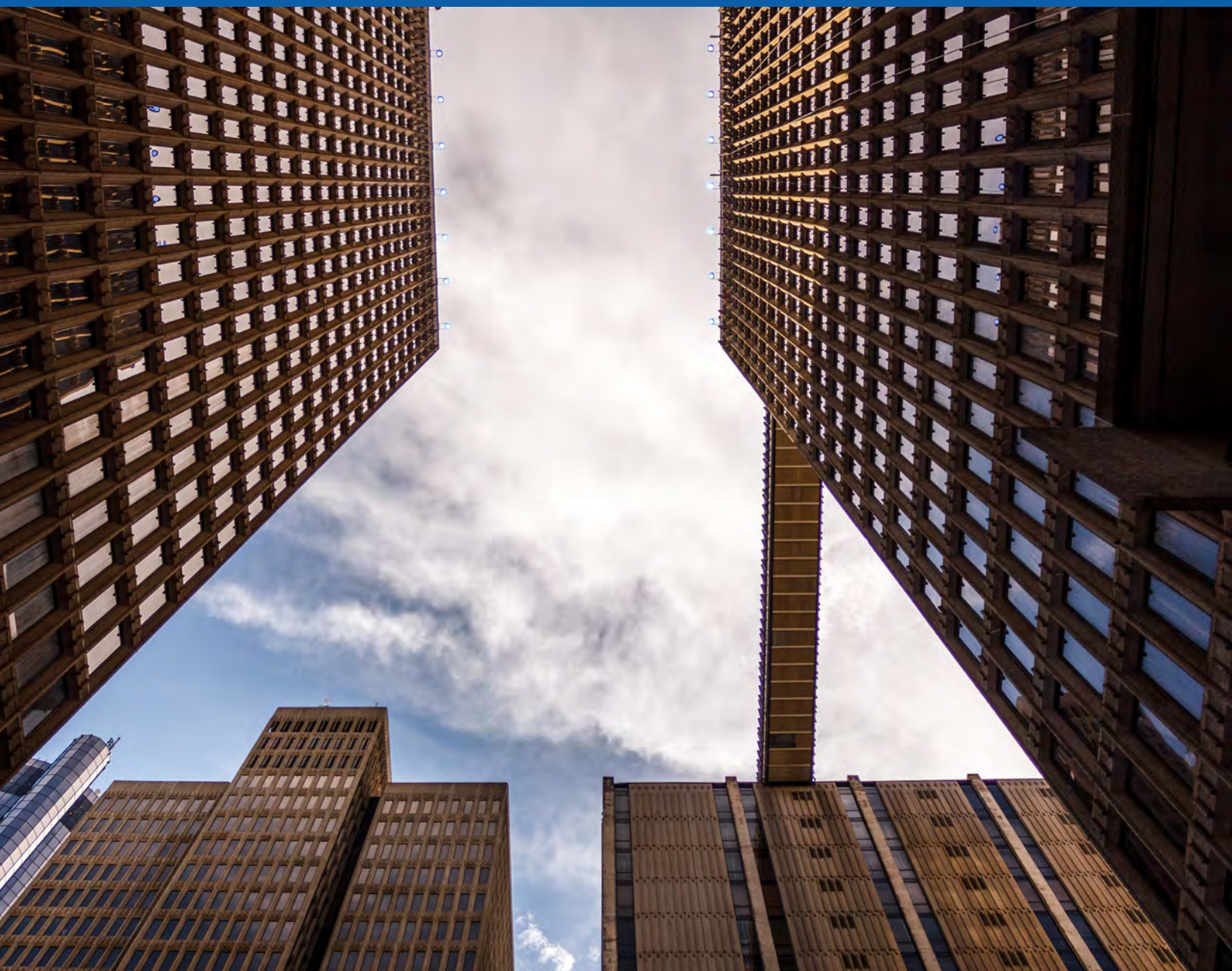
The traditional value-added reseller (VAR) has evolved to a full service value-added solution provider, which offers valuable procurement and management support for enterprise security teams.

APPLYING THE CONTROLS

The practical usefulness of the fifty-four TAG Cyber security controls has been validated since 2016 by many enterprise teams who use the framework to identify gaps and optimize the selected controls for their security portfolio. The TAG Cyber team recommends that portfolio managers and consultants who assist enterprise teams with vendor selection make full use of the structure.

Ultimately, each enterprise will have to tailor its security architecture to its unique needs. Lager organizations, for example, will rarely need unified threat management (UTM) gateways for smaller networks, and companies that have little creative video, music, or written material will rarely need content protection. In general, however, the controls provide a useful guide for enterprise teams to measure the completeness of their program.

At the most basic level, portfolio managers would be wise to map their projects, vendors, and deployments to the TAG Cyber controls to get a general sense of coverage. If, for example, a gap is identified, then this helps drive a new project to identify suitable vendors that can address the missing protection. On the other hand, if the security program matches or is a super-set of the TAG Cyber controls, then this offers evidence that the portfolio managers have done a thorough job.



GOVERNMENT

PROPOSAL FOR A CYBER DEFENSE TO PREVENT NATIONAL ELECTION MEDDLING

A cyber security threat assessment of our national election infrastructure would identify three broad components as requiring protection against nation-state meddling: *Online political messaging* (targeted by Twitter bots), *campaign support systems* (targeted by traditional hacks such as phishing), and *voting infrastructure* (targeted by hackers removing ROM chips from Diebold machines). These are the components.

A cyber security architectural assessment would then identify three corresponding programs to protect these components: National digital risk monitoring (which large companies use to protect their brand), *national cyber defense for campaigns* (which should mirror Secret Service detail for viable candidates), and decentralized voting operations (which must continue to prevent cascading threats).

The result is a pseudo-professional IT and network set-up that results in less-than-optimal security support for campaigns.

Let's start with *national digital risk monitoring:* Large companies now either employ expert staff or hire vendors to monitor their brand, domains, and resources for real-time evidence of misuse on the internet. Special investigative tools are used to pore through social media, online services, and email on a 24/7/365 basis. The overarching goal is to identify cases such as some jerk spoofing your domain to post garbage onto sites like indeed.com.

Behind the scenes of such services are trained cyber experts who interpret collected information, identify unacceptable postings or social media usage, and then work with the principals to mitigate the incident. Our nation needs just such a team of experts, perhaps in a virtual SOC, to do this for our national election systems on an impartial, bipartisan basis. They can cooperate with social media owners to locate and mark obvious junk postings from bots.

An additional benefit is that the Turing tests and content filters used by social media companies such as Twitter would benefit from this national digital risk monitoring. Even the best machine learning tools enjoy some level of human assistance, so their bot detection algorithms would be improved by the security analytics performed by our national digital risk monitoring team. (Just writing about this makes me want to work there.)

Let's move on to *campaign support systems:* Everyone knows that the size of political party staff swells before elections and then deflates afterward. The result is a pseudo-professional IT and network set-up that results in

less-than-optimal security support for campaigns. We all cringed at Mr. Podesta's handling of emails, and we all cringed further at the poor incident response processes in place at the DNC. It was a disgrace.

What is needed now can be derived from something we already have: That is, when a candidate is approved for Secret Service detail, their campaign's entire IT and network operation should be forklifted into a protected enclave run by experts with NSA heritage. Campaign iPhones should be smashed, existing systems burned, and office space boarded up. Each campaign's IT systems should be rebuilt in a SCIF-like system operated by experts.

This is not a tough thing to do, by the way. For example, the IC figured out long ago how to do cloud computing; they just do it in a classified playground. The idea that our national campaigns would become temporary tenants in a super-high assurance, intensely-monitored computing environment is no more jarring than starting your first day as an employee at Ft. Meade. You get new stuff and you learn new procedures. You adjust. It's no big deal.

Now, some might say that massive insider leaks would come from such a network. Well, here is how a professional CISO would respond: The best way to prevent leaks, any CISO would tell you, is to follow a code of conduct that involves never typing anything stupid or mean or ridiculous ever. Every CISO on the planet – and I mean *every CISO on the planet* – tells their executives (and I quote): "Never put anything in email that you wouldn't want to see on the front page of the New York Times."

Finally, let's consider *voting infrastructure:* As a computer security expert, I can vouch for the fact that machines from companies like Diebold can be hacked. Avi Rubin from Johns Hopkins University, for example, could probably show you a hacking demo of an ES&S or Sequoia that would make your toes curl. So, if we expect to connect all of these insecure devices into one, large national electronic voting network, then good luck with the security of that monster.

Instead, we must reaffirm the distributed power of local, regional election systems. Sure, we can debate whether home voting is better than election places, or whether better identification is required for our citizens. But these are non-cascading problems. Issues in one neighborhood, for example, cannot electronically spill over into another neighborhood, or city, or state. Distributed local voting is a good idea from a cyber security perspective.

In case you remain unconvinced, I had the wonderful pleasure to interview both Whit Diffie and Ron Rivest – the Henry Ford and Thomas Edison of cryptography – on what they thought of using, for our elections, the high assurance PKI-based protocols and systems that they invented. Both men answered unequivocally that we would be better off using paper. Now, I think you will agree that if these guys don't trust national networks for voting then we shouldn't either.

A professional cyber security operations manager would certainly ask what sort of budget would be required for these three programs. In the context of what we've spent as a nation dealing with the aftermath of reported attacks during our last election, these three initiatives would be super-inexpensive bargains, probably totaling about 200 million dollars per year. That's about half of what we spend on Big Bird. We should set aside the money and do this now.

By the way, the true litmus test is how our adversaries would respond to such a three-pronged program of national election cyber defense. I expect that they would shrug and say that anything can be hacked, and they would brag that they can breach any network, including one run by NSA-types. But let's face it: When the cameras are turned off, and our adversaries retire to their private quarters to contemplate what we are doing, they would be pissed.

And that is precisely what we should hope for as we plan a system of cyber defenses for our future national election infrastructure.

A SUGGESTION FOR THE FBI ON CRIMINAL PURCHASE OF CREDENTIALS

I have a suggestion for the FBI. It's related to credential theft by criminals trying to make money through email and calls. This contrasts with nation-states nabbing credentials to support their military, as we saw with those PLA members indicted by William Barr.

Now, if you are wondering why I would post my suggestion here versus running over to Federal Plaza – well, it's this: My proposed prevention method works best if everyone knows it's happening. By the way, that's a nice (but rare) security property if you can get it.

Oh, and this: Many of you will hate my suggestion, perhaps intimating that it will be intrusive of privacy, and that the FBI will overstep its bounds. That may be true, but we all know that credential theft is growing. I'm merely suggesting a way to reverse the trend.

When you can nab those Uber riders or T-Mobile users for a fraction of a cent per record – well, the temptation to break the law might be too much.

Here's the concept: When credentials are stolen and popped up on the Dark Web, certain nefarious companies buy the lists for cheap Bitcoin and then contact the entries to sell them something. You'd buy stolen T-Mobile credentials, for example, to hawk phone cases.

Some recent prices: In November 2015, 590,000 Comcast customer records could be bought for $1,000.00. In March 2016, you could buy 1.5 million Verizon customer records for $100,000. In November 2017, 45 million Uber records were also on sale for $100,000.

Unless you're under a rock, you know it's easy to spot which companies are mass emailing or call-marketing. And I take no issue with the mailers or other tools they use. What I would like to know instead – and what the FBI should probe – is where they obtained their lists.

Businesses thrive on contact lists. And the correct way to build lists is to do the legwork, or presumably to buy them legally. But when you can nab those Uber riders or T-Mobile users for a fraction of a cent per record – well, the temptation to break the law might be too much.

Here's where my suggestion comes in (and now I'm talking to the FBI): First, you will need an automated means to identify mass senders and robocallers. ISPs could provide the data in real-time. The marketing platform companies would be better – so you also could try there.

The other option is to just build the list of mass emailers and robocallers through your own investigative means. I'm going to go out on a limb here a bit and guess that you already have this information. It's not terribly hard to obtain through simple automated methods.

For you FBI lawyers, I know you're thinking that legal basis must be established for demanding or grabbing this information. Given the negative impact that stolen credentials and mass marketing have on society, I think this will be a straightforward case.

Now, once you (the FBI) have access to your targets, you can auto-issue these mass senders a request (er, demand) for proof-of-purchase of the contact list they are using. If they respond that their contacts were built organically, then randomly audit that process.

Again – the tool being used is irrelevant. The seller might be using a mass emailer or a customer relationship management platform. You don't want the receipt for that. You want the receipt for the customer contacts. Pipedrive or Salesforce don't come pre-populated.

In the beginning, you will experience some turbulence. You'll send your notifications to the wrong companies, perhaps out of your jurisdiction. You'll get bounce backs. And you will probably scare the wits out of some church group sending notes to their parishioners.

But after a fashion, I think you will like the effects of this process. Nefarious companies who are considering using Tor to purchase a million stolen credentials might just think twice before pulling the trigger if they know you are coming. It's not perfect, but no security is.

I hope you take my advice, and I'd share my contact information if you want to discuss this further, but we all know this is not necessary: I'll wait to hear from you. For the rest of you on social media who've trudged this far into the article, let me know what you think.

But please, please remember to be extra careful before you post any nasty criticisms or mean-spirited comments on this article: The FBI might be listening.

Have a nice day.

WHY CHINA PRODUCES NO MEANINGFUL CYBER SECURITY START-UPS

During the past four years, I cannot recall a single meaningful discussion with a cyber security start-up founded in China. And this is not for lack of trying. At TAG Cyber, we have no policy to avoid countries in our assessment of cyber security vendors. Despite this, I can report that I've found nothing interesting to date. And yes – I know that Huawei and ZTE list cyber security as capabilities on their websites, but neither are security vendors.

This might seem surprising, given the vigorous attention China has placed in adjacent high technology markets. Witness those cool electric SUVs coming off those intelligent, automated assembly lines in Wenzhou. And check out the amazing (and terrifying) facial recognition systems that capture people jay-walking in Shenzhen. And don't forget the recent innovations being accelerated (uh, tariffs) in Chinese semiconductor firms like SMIC.

> They simply do not have much of an embedded, legacy base of companies with poorly managed systems, because they don't have much of an embedded, legacy base of business.

So, it's unreasonable to suggest that cyber security start-ups are missing from China due to Luddite culture or lack of capital. This cannot be the reason. Instead, our analysis at TAG Cyber suggests a somewhat different explanation for this unusual gap. By looking carefully at the social conditions that would seem to nurture the development of cyber security start-up founders, we've identified three factors that might help explain this phenomenon:

MISCHIEVOUS YOUTH CULTURE – We discover in our work at TAG Cyber many security founders, especially in the US and Europe, who developed an interest in cyber-related issues during a mischievous youth. We hear stories every day from edgy young founders who poked around in places where perhaps they should not have, only to find that this yearning to explore, and even break the law (ahem), would be a useful tendency for cyber security.

Now, I am no psychologist, and I cannot provide a comprehensive commentary on youth culture in China. But as an NYU and Stevens professor of computer science for decades, I've come to meet many hundreds of young people who grew up in China. And I can tell you that they never, ever tell me stories of brazenly breaking the law as youngsters. In contrast, American students brag their stories of mischievousness all the time.

CONTINUOUS THREAT AWARENESS – We also find in our work at TAG Cyber that many cyber founders honed their technical skills in an environment which included consistent societal awareness of an imminent and present threat. Israeli founders win the prize here, and we are treated to stories literally twice per day of cyber executives – young and old – who are driven by a culture of country threat, often reinforced by time served in the military.

Once again, during decades of many wonderful Chinese graduate students in their early twenties answering questions about Kerberos on my midterms, I don't recall ever hearing stories from these youngsters of growing up in constant fear of foreign attack – and admittedly, US students rarely offer this view (most were toddlers in September, 2001). Again, this might be anecdotal, but it seems relevant to the lack of Chinese cyber start-ups.

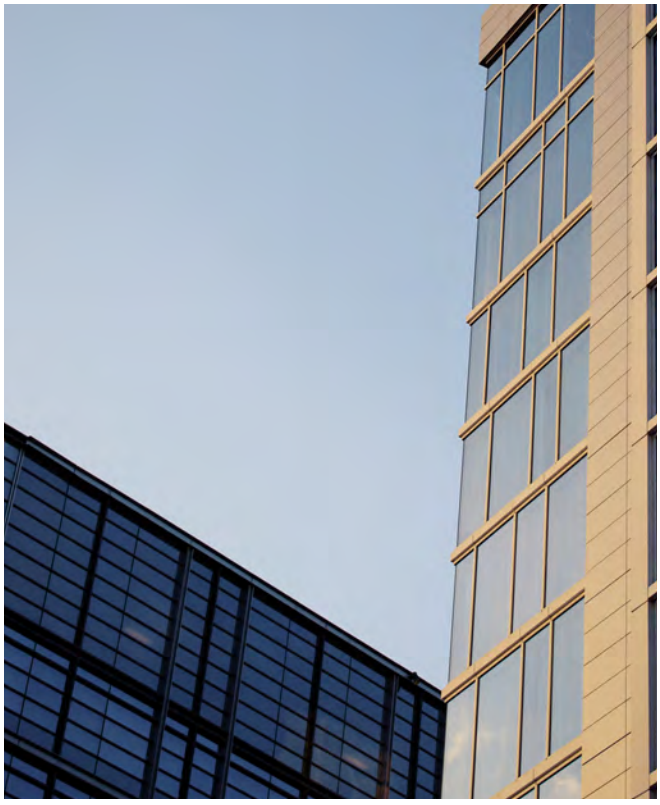
ENTERPRISE LEGACY VULNERABILITIES – A third observation from our work at TAG Cyber is that many cyber start-ups build business cases on the nagging, legacy vulnerabilities in existing corporate and government infrastructure. They point to weak corporate LANs, misconfigured firewalls, uninformed employees clicking on phishing links, and on and on. These legacy enterprise weaknesses fuel platform sales and help start-ups get off the ground.

In contrast, China is building the canonical leap-frogged infrastructure with focus on brand new 5G-powered networks. They simply do not have much of an embedded, legacy base of companies with poorly managed systems, because they don't have much of an embedded, legacy base of business. Capitalism is a relatively recent phenomenon, so one is more likely to hear about issues with mobile devices than with legacy firewall-based LANs.

Now – before you start typing in your angry protest, showing me the dozen or so cyber security companies like Sangfor that popped up in your Google search, let me comment: I did not say that there were no security start-ups. I understand that there are Chinese companies building AV and NAC, and other traditional solutions. What I said instead was that I could find no meaningful cyber security companies. And I stand by that point.

Despite all this, perhaps the *real* reason – the honest reason – that China barely scratches the surface in the cyber start-up ecosystem is that their government knows that it cannot dominate this area. With the Israelis and Americans so far ahead, one can only imagine the planning sessions of Chinese leaders. *Why focus on crowded markets like cyber, they have likely concluded, when you can dominate AI, solar energy, and electric cars?*

Why is this relevant? Well – as the United States and other countries continue to develop their long-term strategies for protecting critical infrastructure, the idea that China has largely punted in developing their own cyber defensive offerings should factor into the planning discussions. Sadly, the United States has such poor leadership in this area (witness, no Cyber Czar) that this observation might not have been made in Washington. Hence, my article.



I hope that you forward this article to your government representative. They seem happy to go on Fox News, CNN, and MSNBC to complain about Chinese Trojans in Huawei equipment, or in Chinese investments in American companies. But no one seems to mention this other thing – namely, that virtually 100% of the cyber protections built to defend against cyber threats – are invented, developed, and maintained by companies outside China.

I understand that this might have been a somewhat edgy article. Let me know what you think.

A PROPOSED CYBER SECURITY TRANSITION PLAN FOR THE NEXT PRESIDENT

This note proposes a six-month plan for the next US President to create a fresh national program of cyber security readiness, protection, and response. I offer this plan four months in advance of the election so that transition teams can benefit from the ideas included.

Before reading my proposal, please recognize that positions, committees, and documents are worthless if they are not used. Trump's existing National Cyber Strategy, for example, has had zero impact on anything meaningful. Americans can do better than this.

Here is a detailed schedule of what I would recommend to the next Administration to get us back on track in protecting our nation from cyber threats:

Please recognize that positions, committees, and documents are worthless if they are not used.

NOVEMBER 2020

INTERIM TRANSITION COORDINATOR FOR CYBER SECURITY (ITCCS) – The new President-elect should appoint an ITCCS to handle national cyber security policy priorities and to begin reviewing existing cyber security-related programs in the present Administration.

OFFICE OF THE DIRECTOR OF NATIONAL CYBER SECURITY (ODNCS) – The ITCCS should present a proposal to the President-Elect for an ODNCS position to replace the Trump-dismantled Cyber Security Coordinator slot pioneered by Howard Schmidt under President Obama.

BUDGET PLANNING – The ITCCS should begin to prioritize all department and agency budgets in cyber security with priority for initiatives that enhance defensive posture, support cyber innovation, and train next-generation Americans to protect critical infrastructure.

DECEMBER 2020

TRANSITION REVIEWS – The ITCCS should coordinate a recruited team of experts to begin the transition-related meetings and reviews with DHS, NSA, FBI, and related departments and agencies that have cyber security responsibilities in the present Administration.

NATIONAL CISO ADVISORY COUNCIL (NCAC) – The ITCCS should appoint and convene an NCAC to provide ongoing guidance and feedback from actively working CISOs to the Administration on cyber security matters related to enterprise protection.

JANUARY 2021

TRANSITION TO ODNCS – All cyber security initiatives should be transferred to the ODNCS after the inauguration. The ITCCS should recommend a carefully prepared short-list of ten candidates (from a target list of 200) to the President for the DNCS position appointment.

OFFICE OF INTERNATIONAL CYBER SECURITY COORDINATION (OICSC) – The DNCS should create a new OICSC to oversee all cyber-related coordination, negotiation, and planning with international security government contacts including in China and Russia.

CONFERENCE ON SOCIAL MEDIA PLATFORMS – The DNCS and the President should hold a private conference of technology, social media, and security executives to discuss meaningful laws to prevent fraud, abuse, and misuse of social media including Facebook.

CYBER SECURITY RECRUITING AND RETENTION – The DNCS and the President should convene a virtual conference of all federal cyber security workers to request their continued service, regardless of personal politics, and to recruit new experts to join the federal government.

FEBRUARY 2021

PRESIDENTIAL DIRECTIVE ON NIST 800-53 – The President should issue a Presidential Directive stating that the NIST Cybersecurity Framework and NIST 800-53 rev 5 shall be the only framework and requirements to be used in federal cyber security compliance work.

CABINET WAR GAME – The ODNCS should run a cyber war game for Cabinet members. The game should include a worst-case security disaster scenario to highlight gaps in national readiness. Each Cabinet member should provide a follow-up plan after the war game.

WHITE HOUSE IT CISO – The President should appoint a full-time CISO to oversee and manage all IT-related cyber security matters for White House staff. This new white House CISO position should be considered peer-level to the White House Director of IT.

NSA AND CYBER COMMAND SEPARATION – The President should begin the political and legal process to separate the National Security Agency (NSA) from the US Cyber Command. Effort should be made to retain existing leadership in the new Administration.

BUDGET RECOMMENDATIONS – The DNCS should provide an initial budget estimate for all federal department and agency budgets in cyber security with emphasis on long-term return on investment (ROI) and protection of critical infrastructure from cyber threats.

MARCH 2021

PRESIDENTIAL DIRECTIVE ON US CYBER CORPS – The President should issue a Presidential Directive stating that all Civilian Agencies will increase their Cyber Corps students to 500 per year, per agency. Funding should be obtained through large commercial donations.

NATIONAL SECURITY VENDOR ADVISORY COUNCIL (NSVAC) – The DNCS should appoint and convene an NSVAC to obtain relevant ongoing guidance and feedback to the Administration from domestic commercial cyber security technology vendors.

STATE AND LOCAL LIAISONS – The DNCS should identify and coordinate with designated state and local cyber security teams to develop, test, and maintain practical plans for nationwide emergency response to potentially serious large-scale cyber security attacks.

APRIL 2021

PRESIDENTIAL DIRECTIVE ON US FEDERAL AGENCY CISOS – The President should issue a Presidential Directive stating that all Civilian Agencies must present a zero trust-based cloud transition plan for review and approval by the ODNCS.

NATIONAL SECURITY ACADEMIC ADVISORY COUNCIL (NSAAC) – The DNCS should appoint and convene an NSAAC to provide on-going guidance and feedback to the Administration on matters related to secondary cyber security education.

OUR FAILED NATIONAL CYBER DOCTRINE

During the past two decades, a period in which United States politics has swung wildly back and forth between successive Administrations, America has been governed by a surprisingly consistent National Cyber Security Doctrine. Starting with Bill Clinton's Presidential Decision Directive 63 in 1998, and culminating with our current Government's cries of foul against Chinese intellectual property theft, the underlying cyber security beliefs influencing decisions from each White House have not shifted, despite evidence of their stunning ineffectiveness.

The first component of our national cyber security doctrine is the belief that hacked companies and agencies must be punished. The size of the punishment has tended to track closely with the severity and consequence of the incident – but hefty fines, management firings, and even public humiliation have been common post-cyber attack occurrences. The painful image comes to mind of Kathryn Archuleta, Director of the Office of Personnel Management, raising her right hand in shame before a Congressional hearing after her agency's serious data breach.

If one could demonstrate…that the United States has benefitted from this doctrine of victim punishment, adversary warnings, and user lament, then any discussion of change would be moot.

The second component of this doctrine is that preventing exploitation of national infrastructure is best accomplished through expert negotiation and intense pressure aimed at the nation-state sponsors of such malicious activity. This strategy includes the use of warnings and rhetoric from each President, as well as more formal actions such as Department of Justice charges being raised against foreign hackers. The implicitly held view is that *if only these nation-state actors would just stop*, then perhaps America could return to some sort of cyber normalcy.

The third component of cyber security doctrine held uniformly across the last twenty years is that most breaches could have been avoided by common sense. That is, cyber risk might be avoided if only organizations would just share information more freely; and *if only* users would just select better passwords for their Facebook accounts; and *if only* companies would just watch for obvious signs that hacking has commenced. Luddite members of Congress tend to gravitate to these common-sense arguments because they require no technical skill or insight.

If one could demonstrate – quantitatively or even qualitatively – that the United States has benefitted from this doctrine of victim punishment, adversary warnings, and user lament, then any discussion of change would be moot. But by any reasonable measure, Americans have seen a substantive increase in cyber security risk across virtually every aspect of their lives – from personal data losses in non-regulated industries such as social media, to severe breaches of trust from large regulated companies or government agencies handling sensitive data.

What this suggests is that a change of thought is required – and the belief here is that literally inverting our existing views, flipping them upside down, offers an excellent template for the current Administration. Setting aside the obvious concerns with a President who mishandles technology in

the most abysmal manner from a security perspective (consider that no Fortune 500 security chief would ever allow its CEO to tweet sensitive information in the manner of Mr. Trump), the following three adjusted views are suggested to help our nation get on track:

First, the routine punishment of hacked organizations must cease. Cyber security has reached the point where any pick-up game between hackers and defenders will *always* be won by the offense. The implication is that defenders need help – and this requires a shift in cyber doctrine. That is, when a company is breached, the response by our leaders should involve meaningful assistance and thoughtful support. Imagine a building in an American city being strafed by an enemy air attack. Would our response be to fine the owner and humiliate the superintendent?

One can only expect critics to claim that this softer touch would encourage sloppy, lazy cyber security and poor compliance. But this flies in the face of reason: It is in the interest of every organization to improve their cyber security posture. The problem is that this is easier said than done – even for the largest organizations. Conventional wisdom amongst Chief Information Security Officers is that the US, China, Israel, Russia, and the UK could break into any system under even the strictest compliance. We must replace our blame culture with one of support.

Second, we must accept that determined pleading with malicious nation-state actors will not lessen the cyber security threat. Every security expert is quick to point out the asymmetric nature of the cyber threat; that is, consequential attacks do not require significant sponsorship or funding sources. Rather, they only demand the persistence of some clever individuals with sufficient motivation to accomplish a targeted malicious objective. Cyber security lives in the ultimate mouse-that-roared environment, and our leaders need to recognize this fact.

In its place, I'd recommend that we dramatically shift our focus toward truly defending ourselves. Our new doctrine should include the belief that if our country is hacked, then we must all look in the mirror and bear collective blame. Certainly, we must continue to seek and prosecute cyber offenders, but our doctrine should hold that it is our joint responsibility as a nation to self-protect ourselves and neighbors, and that no level of negotiation with Russian or Chinese leaders will lessen the potential for rogue actors to bring down our infrastructure.

Third, our doctrine must be adjusted to accept that cyber security is an enormously difficult task. It requires expert attention to complex technical detail. It requires tools that are intricate in their design and delicate in their operation. It requires trained staff from universities and expert teams in industry who can provide the apprenticeship required for any budding cyber security professional. This belief that cyber security is just one good "Top Ten Tips" compliance poster from stopping foreign attacks is patently ridiculous. Cyber security is demanding.

An implication is that our nation should commit itself toward meaningful promotion of education for our young people in technology and cyber security. President Trump has the great opportunity now to direct significant, additional funding toward our small and fractured cyber corps programs. He should appoint a modern-day Sargent Shriver to excite our youth to follow a career of service to their country in cyber security. It is hard to imagine a more obvious and exciting way to bring our entire country – both red and blue – back together.

A final warning regarding cyber doctrine: Americans have a long tradition of waiting until after an attack occurs before springing to action. Pearl Harbor and 9/11 are cases in point where we napped quietly until nudged. While this romantic view might make good script, I would warn that cyber security is a different animal. If our country's power, water, food, communications, and transportation are suddenly yanked from our control, then we might not have the response tools or national resolve required to fire a successful cyber Hail Mary after a serious attack.

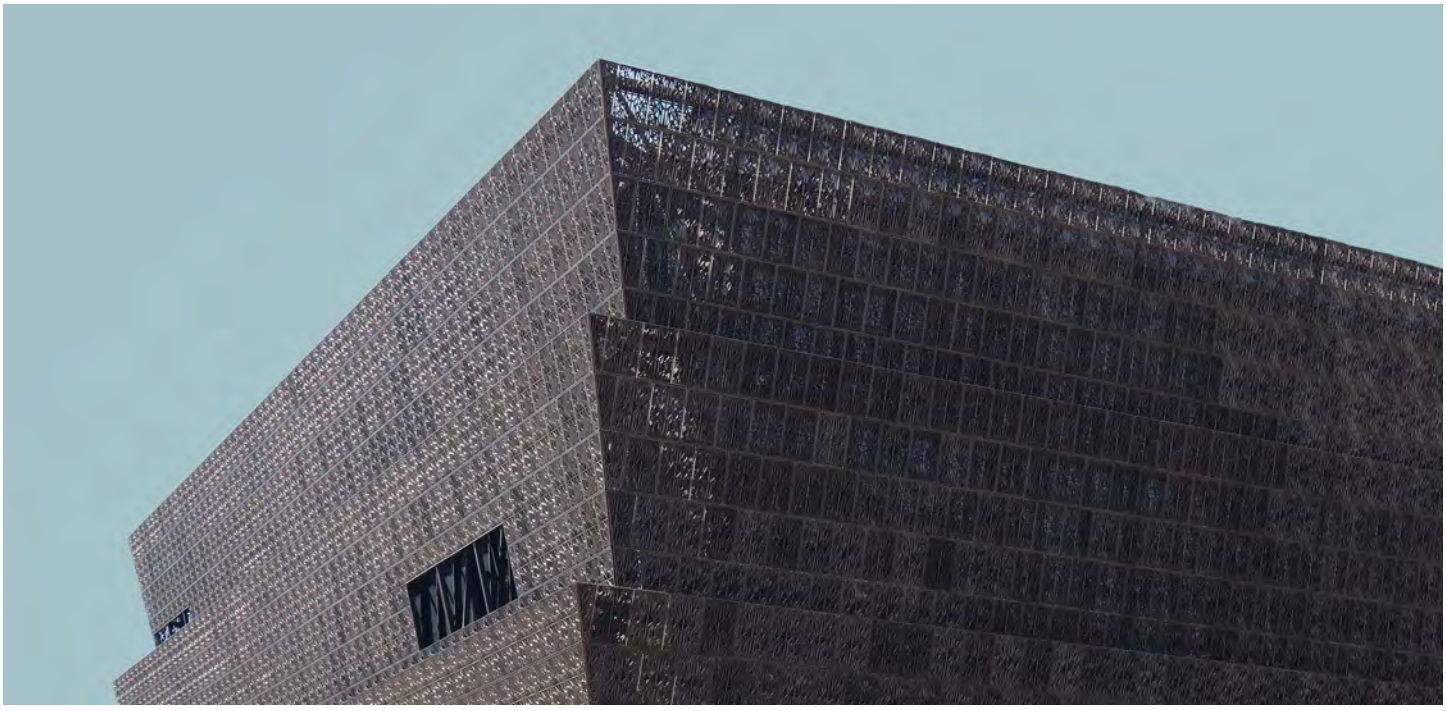
WHAT TO KNOW BEFORE MOVING FROM GOVERNMENT TO INDUSTRY IN CYBER

This article was shared with the community to help those cyber security professionals moving from government (usually Federal and often military) to commercial industry positions in cyber security. The article tends to focus on United States Federal Government employees, but the discussion can easily apply to others. Members of the Israeli Defense Force, for example, move frequently from public service to industry positions, often in cyber security start-ups.

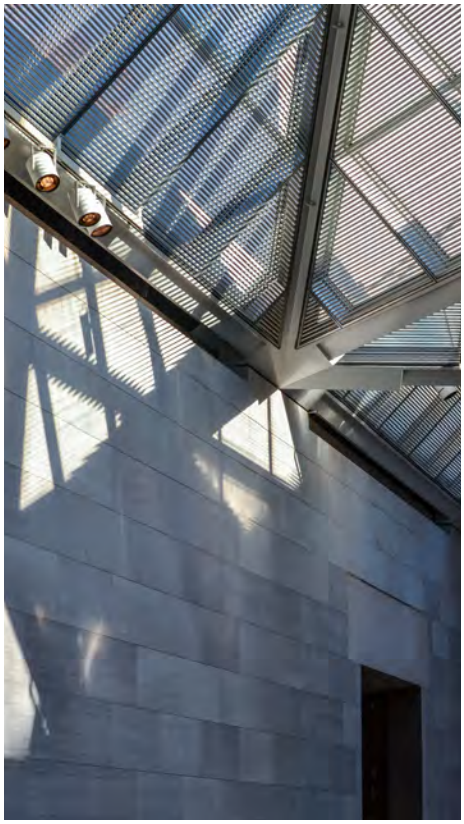
In the shadow of Andrew Jackson's statue near the center of Lafayette Square in Washington rests one of the most famous benches in American history. Officially dubbed the *Bench of Inspiration* fifty-nine years ago, the small resting place is where the great financier *Bernard Baruch* held private court with the leaders of our country during the 1940's and 1950's. The bench remains today a symbol of public-private cooperation in the US.

The successful security executive coming from some federal department to a power or retail company had better learn to identify the company's business objectives.

That business leaders should step away from industrial management to serve their fellow citizens is well-established in our nation. Sometimes it results in the gift of capable insight, as with Mr. Baruch serving many presidents including FDR. And other times the results are more questionable, as with the *Whiz Kids* from the Ford Motor Company using modern dispassionate accounting methods to help justify LBJ's continued involvement in Vietnam.



Regardless of the outcome, the move from industry to government remains popular, and continues to allow executives to give back to their country. More modern examples of this transition include Perot, Trump, Corzine, Romney, Whitman, Forbes, Bloomberg, Fiorina, and on and on. Each of these individuals transferred executive skills learned in industry to become political leaders (some more successful than others, obviously).



But what of the reverse move? The transition from government to business has been less welcome – even considered unsavory at times. Images of former political leaders taking money for speeches to companies are met with great scorn by citizens, as if some crime were being committed. Even the nomenclature used is weird: Government leaders will say, for example, that they are moving to the private sector. No one in business uses that term.

This issue is especially relevant in our cyber security community, because the reverse career move from government to industry for CISOs is not only common but encouraged. Boards, C-suites, and investors laud the idea that someone federally-trained in cyber security would come to industry to leverage their experience. Few people question the potential success of such moves, and as far as I know there have been no studies to see if it works.

I can tell you, however, that many CISOs with government experience have had bumpy dealings with cyber threats. *Sony Pictures, JP Morgan Chase*, and *Capital One*, for example, all experienced serious data breaches with government-trained security executives at the helm. These cases might be coincidence, but they do prompt the question of whether the transition in cyber security from government to industry is being properly managed.

Based on four decades watching this process unfold, including my own very brief stint serving government in an official cyber security role, I can offer three suggestions for any cyber security executive doing the shift to the private sector (ahem). I should preface my comments by saying that these are intended for executives moving into operational roles in cyber defense. Government experts doing start-ups should look elsewhere for advice.

The first suggestion involves the *means* and *purpose* guiding the day-to-day work of the CISO and security team. In government, both the means and purpose will consist of this: *Meetings* with the right attendees, documents with the right content, and *councils* with the right organizations. If you check each of these three boxes, you will be a successful civil servant (and admittedly this is less true in the military as in civilian government).

In industry, things are a bit different. Any business executive will tell you that meetings, documents, and councils are to be avoided wherever possible. They are neither the preferred means nor the target purpose for any initiative, much less ones related to cyber security, where long meetings and boring reports are loathed. Every CISO in industry knows, for example, that number-of-meetings is booked on the cost side of the ledger, not the reverse.

Successful businesses focus instead on tangible results, and this is often accomplished through simplification. Interestingly, in many environments, such simplification can be achieved by dramatically reducing the number of . . . yes, you guessed it: Meetings, documents, and councils. The successful security executive leaving a civilian agency to join a bank had better learn this fact quickly – or prepare to relocate back to River City.

The second suggestion involves how an individual's job performance is evaluated. In government, every federal CISO or security executive knows that *fairness* is the primary metric by which civil servants are compared and compensated. The United States Office of Personnel Management publishes a guide that lays out the basics of this process, which boils down, more or less, to making sure that everyone is treated the same.

When managers depart government and land in a business, however, they quickly realize that when it comes to performance review, the concept of fairness is interpreted quite differently. That is, it is considered fair to treat higher performers better than weaker ones. This can include visible recognition such as trips to Hawaii or the best corner offices. Unlike in government, *fair* does not mean *same-for-all: Fairness* is based on merit.

What this means is that the successful security executive coming from some federal department to a power or retail company had better learn to identify the company's business objectives. And all job performance activity had better link directly to the practical achievement of those objectives. Do this properly, and you will advance. Do it poorly – and, well . . . you might be back in that cubicle in Arlington tapping into a slow Windows PC.

The third suggestion is perhaps the most difficult for anyone coming from government to accept. Recognize that federal cyber security teams, especially in the military and intelligence communities, are driven by a passion to serve their nation. The stark recognition that global cyber threats from an adversary could impede one's way of life, helps to drive this passion – and we all benefit from such fine motivation. It is wonderful.

In stark contrast, however, modern business executives in public companies are coldly driven by three quantifiable objectives: *Earnings, stock price,* and *growth*. This is neither good nor bad. It is just *different* from the underlying factors that motivate federal workers. Businesses must do whatever needs to be done to optimize these factors. Their only recognized adversaries are competitors: Coke doesn't hate foreign hackers. They hate Pepsi.

The successful security executive coming from government must therefore learn quickly that protecting one's nation is not the charter of business – unless their products or services are used for such purpose. And yes – corporations can be good citizens and can help during times of stress such as terrorist or weather emergencies. That said, an enterprise will go out of business if it doesn't focus on its stakeholders.

I hope security executives who are either planning to move from government, or who have recently done so, will take my advice to heart. Partnership between the public and private sectors requires close coordination, and the cross-pollination that comes from executives making this switch helps lubricate this process. We should all encourage movement in both directions between business and government.

But the government security executive who is trained to use meetings, documents, and councils in an atmosphere of employee fairness, with the ultimate goal of protecting society, might be in for a rude awakening. In business, the successful executive minimizes the number of meetings, documents, and councils, in an atmosphere of rewarding merit, with the ultimate goal of making lots and lots of money. It's not better or worse: It's just different.


ENTERPRISE

THINKING OF JOINING A BOARD? READ THIS FIRST.

With so many cyber security professionals – especially Chief Information Security Officers – having intense interest in joining corporate boards, this article seems particularly important. Its main premise is that not everyone (including the author) is always well-suited to particular boards. The article offers three questions that potential board members should ask themselves before agreeing to serve as a director on any board.

Let's begin with the disclaimer my attorney demanded after nearly fainting from an earlier draft: "All statements made here are hypothetical, and in no way reference the appointments, elections, or involvements of your naughty author on any corporate, government, or academic boards. This is a made-up work designed to incite social media collisions. If you are a squeamish board secretary, then please look away."

Before you join any serious board, you should first determine whether you have the right personality to put up with the slow and tedious process of governance.

Now that the legalese is covered, I'll share the basic thesis of my essay, which is this: Before you join any serious board, you should first determine whether you have the right personality to put up with the slow and tedious process of governance. I am not one of these people – and I've either quit or allowed my seat to elapse from every decent board I've ever been invited to join. Below I will explain why – and hopefully help you avoid my mistakes.

To start: Many executives seem to excel at board work – or at least, it looks that way. They glide so smoothly into meetings, inject safe and friendly questions at just the right time, and prompt the delighted chairperson to cast over that occasional knowing glance to confirm that the board member is just so appreciated. It's an amazing thing to watch – and I have no idea how they do it. If you are one of these people, you have my jealous admiration.

Surprisingly, at least to me, many of these successful board members are security executives. My good friend Chenxi Wang from Rain Capital recently penned an excellent Forbes article about how boards are benefiting from the participation of present or former CISOs. From her narrative, the transition from senior management team to corporate board looks as natural as a Veep running for President: More of the same, but just at a higher level.

But beware: There are executives like me who do not excel at board work. They do not glide smoothly into meetings, and they tend to inject unsafe questions at the worst possible time. They frequently make the room cringe as they jab at fancy consultants during presentations. And they never get warm-and-fuzzy glances from anyone. It's a terrible thing to experience, and if you are one of these types, then you should avoid boards – hence this article.

I offer below a little self-test that you can use to determine your suitability for board work. I should preface my remarks, however, with this point: My focus here is on paid board positions with fiduciary responsibility – where you wear a suit to meetings and get your picture in the annual report. I am not talking about unpaid tech start-up boards where frisbees are tossed around during lively debates. Got it? OK – let me explain the self-test.

During many years of direct and indirect involvement with boards on both sides of the briefing podium, I've had a front row seat to observe and learn the types of personality traits that seem well-suited to governance, as well as ones that do not. I've codified my observations into a three-question test and associated rubric that are designed to expose these traits. None of this is based on empirical or collected data: It's all from my head.

But recognize that my experience is vast: In additional to personal elections and paid appointments on a variety of corporate, government, academic, technology, and even community boards, I'll bet I lead the league in invited presentations to boards on cyber security. I even tag-teamed a board presentation once with Bob Mueller just months before he became Bob Mueller. So, rest assured that I'm not just pulling this from Google.

I also fully understand the scope, focus, and purpose of the board member. I've sat through the training, read the workbook materials, and gone to the conference sessions. I know that the board director's purpose is to ensure the organization's prosperity by collectively directing the company's affairs, whilst meeting the appropriate interest of its shareholders and stakeholders. (OK – I got that definition from Google, and who still says whilst?)

So, take a few minutes and read the questions below. If you find that you answer "yes" to all three, then please find something else to do in your retirement. Volunteer at your church (stay off their board, though), or take the grandkids fishing, or whatever. But if your answers below suggest the kind of restless energy that made me a total crap choice for board work, then beware if you get that tempting call to serve. Here are the questions:

SELF-TEST QUESTION 1: DOES YOUR BRAIN EXPLODE IF A SMALL, BUT INCORRECT DETAIL GOES UNMENTIONED?

It has been my observation that good board members (and again – I am not one), have the ability to just let some things go. Most board meetings are long, especially those two-day retreats. So, when some detail is wrong, a good board member knows that pointing this out is often just not worth the trouble. I have no idea how they do this, and if you think you can do it – then you might just be a good board prospect.

Here's a hypothetical example (that I made up): Suppose that (hypothetically) you were in a board meeting where a paid consultant was displaying your customer satisfaction scores. An unlabeled line is shown on the screen with positive slope, so one guesses that this must be good. But it gets better: Another unlabeled line then pops up just a micron below the other one, that is purported to show the inferior average of your top ten loser competitors.

So, tell me – dear reader: What would be your response? Any data analyst knows that if the average of your top ten competitors produces a line just under your own, then it is likely that you are not first, but sixth (think about it for a minute). If this just doesn't seem all that important to you, and you can just let it go, then this is a good sign of board-worthiness. I can tell you that I cannot let such things go – and this drives chairpersons to drink.

SELF-TEST QUESTION 2: DO YOU GO NUTS WHEN SOMETHING THAT SHOULD TAKE A DAY TO COMPLETE ACTUALLY TAKES A YEAR?

It has been my observation that good board members have the ability to relax and not worry about whether milestones are being reached with any level of urgency. Meetings usually happen monthly, so there is a good chance that some board issue left hanging during one session will sit for at least thirty days before the next little zot of progress. They might glide forward slightly faster in a committee, but you get the idea.

Here's another hypothetical example: Suppose that you were in a board meeting where it was suggested that greater transparency was needed to gauge employee satisfaction and that reviews were needed about work-life quality. Suppose further that the decision was made to create a committee (ouch) to look into the matter – which is estimated to require a couple of months of work. Add the image of board members nodding at this reasonable suggestion.

Now – if you are like me, smoke pours from your ears at such a thing, and you interrupt the discussion to suggest that everyone just hop onto Glassdoor with their iPhones ("Hop onto what?" the chairperson might growl). Imagine the fun when everyone sees instantaneously that your organization averages two stars out of five. Such live derailing might sound responsible to you, but board secretaries gulp down packs of Tums when it happens.

SELF-TEST QUESTION 3: ARE YOU UNWILLING TO TRUST MANAGEMENT BASED ON A HIGHLY CURATED VIEW?

It has been my observation that good board members have the innate ability to be calmly satisfied with those sterile, curated spreadsheets and PowerPoints that telephone-tag their way from the worker to the boardroom. And these directors know full well that these charts were pruned carefully to tell a story, and that unless something truly extraordinary is occurring, the story will be a damn good one.

Here's their secret: They are willing to trust management. When asked about the stream of curated stuff, they will laugh and tell you that management is capable, and that it is the role of the board to support their success. This comes with a nice side benefit: Good board members never read prepared materials

in advance. This is a newbie mistake (guilty!) and one learns quickly to never enter the boardroom with yellow stickies on one's binder.

Look – I could never extend this level of trust to any management team, because I do cyber security for a living. Heck, I don't even trust my mother (with computers, I mean), so there is just no way that I'm willing to grin and bear all the curated stuff, under the presumption that management has everything under control. I just cannot do this – but if you can, then perhaps you can slide into a director role at some point in your career.

I feel obliged to reiterate my legal claim: The above comments are not intended to resemble my direct personal experiences but are designed instead to paint a broad picture. And yes – I can already see the primary comment template that will be posted in response to my article: "Every board is different," the poster will post, "and our board does not function this way." If this is true, then congratulations. But recognize that you are an anomaly.

I also expect to read commentary that restless people like me should suck it up and remain on boards. "The problem with corporate governance," some will post, "is that people like you don't remain on boards where you can hold management to task." Well – I plead guilty to this one, and believe me – I have tried. So, yes – if you like running headfirst into concrete walls, then ignore my advice and go sign the fiduciary paperwork.

A final comment I expect to read is most uncomfortable: "I am a board member," some will write, "and I take offense to your snarky essay. I work closely with management and try to provide sound advice on governance and strategy." To this post, I offer this: If you enjoy board work, then I suspect you possess the calm, relaxed, and trusting personality that some of us were not born with. Thank you for your service – and keep up the good work.

Here's the bottom line: If you answered yes to my three questions, then I really, really, (really) recommend that you pause before accepting a board appointment: Based on my experience (also known as getting old), you are probably not cut out for it. Oh – and every board secretary in the world should send over a thank you card, because my advice will shorten their tedious meetings and keep the chairperson beaming. Happy Board Work.

As always let me know what you think (in a non-curated manner, please).

REDUCING ENTERPRISE CYBER RISK DURING COVID-19

This article was shared with the TAG Cyber community during the earliest days of the COVID-19 Pandemic in early March of 2020. The suggestions made then are still quite applicable, so the article is re-shared here with our readers in the hopes that the ideas are helpful. Working from home via remote access will continue to dominate the enterprise landscape for many years, so security teams must learn to adjust.

With COVID-19 now revving its engine, I suspect that many of you are reading this article from the kitchen table, perhaps still in your pajamas. But even before the present global virus situation, this casual teleworking image was pretty familiar for many job functions. I mean – let's be honest: Checking email is checking email – regardless of whether this mindless task is done on the corporate LAN or across your home broadband.

When an entire company decides to collectively embrace telework at the same time, over an extended period of time, the result is that business processes must change.

But when an entire company decides to collectively embrace telework at the same time, over an extended period of time, the result is that business processes must change. And whether a given change is good or bad is perhaps beside the point (although most required changes to accommodate virtual work are good). Rather, I choose to emphasize that as a result of COVID-19, some business processes will necessarily change. This is unavoidable.

Which brings me to cyber security. Now, it's difficult to make general statements about our proud discipline of protecting enterprise that will apply in all instances, but here is one you can take to the bank: *Business change creates seams between people, processes, and technology that can be exploited.* This is universally true, regardless of how well any business change is managed. The goal is thus to minimize the size and duration of seams.

The conditions caused by COVID-19 are especially dangerous for cyber security, because the changes prompted already have three strikes against them: First, the situation was unplanned, with little or no advance warning. Second, it is largely unprecedented for most workers (I am in my upper fifties and other virus outbreaks felt much different). And third, it has no clear end. Virtual operations are being planned and there is no expiration date I am aware of.

So, enterprise security teams must deal with these exploitable vulnerability seams arising from business process changes. And they must do so for an unprecedented issue that could continue for some time. Sigh. Those are the facts, and if you work in enterprise security, you would be wise (even if your personal politics might suggest otherwise) to take this situation seriously. Below are five recommendations from the TAG Cyber team for immediate action:

ACTION 1: PROVIDE COMMON SENSE GUIDANCE FOR EMPLOYEES ON VIRTUAL CONFERENCING. While most employees already know that Zoom is not just a Seventies kid's show, they should be reminded to be extra vigilant of scamming, eavesdropping, and other threats. Sending a clear text invitation over email to a conference call that will discuss next week's reported earnings is just – well, you get the idea. Remind people to not be stupid.

ACTION 2: DEMAND INCREASED SITUATIONAL AWARENESS FOR SECURITY STAFF. I know that you already tell your boss that you're at DEFCON 1. Despite this little white lie, get your SOC team or other individuals tasked with real-time detection, prevention, and response, and push them from DEFCON 3 to DEFCON 2 (I'll let you fill in the definition). One idea might be a daily stand-up meeting (er, conference call) to discuss real-time indicators.

ACTION 3: REINFORCE SECURITY POLICIES FOR TELEWORKERS. This assumes (I hope, I hope) that you already have a published security policy for teleworkers. If you don't have one, then have a look at this nice guide. It's important, for example, that your employees remember that the helpful teenager at the Apple store is simply not authorized to work on your office computer. Make sure employees know your policies and understand their importance.

ACTION 4: REMIND EMPLOYEES OF HEIGHTENED PHISHING RISK. Everyone knows that when you get stressed, rushed, or confused, you will be more likely to click on something bad. It is your job as an information security professional to remind remote workers freaked out about COVID-19 to please . . . slow . . . down. Remind them that notifications will not come as emails with links. And if some external entity sends such a thing, they should ignore it.

ACTION 5: MAKE SURE YOUR SECURITY HOTLINE IS WORKING. When someone in the office becomes concerned about a security issue, they have the luxury to ask a colleague what to do. When that same person works from home, they are more likely to say the hell-with-it. You can minimize this by ensuring that your security hotline (you have one, don't you?) is working. If an employee sees something suspicious, they should be encouraged to report it.

Look – I know that people like Elon Musk are calling this whole thing dumb – and for the average person, it is probably reasonable that they remain calm and go about their lives in a normal manner. But when you are in a position like enterprise security, it is your job and your responsibility to do the worrying so that others don't have to. The last thing on this entire planet that your company needs is to get hacked as a result of COVID-19.

So, stop reading this article and go start working immediately on the five actions I recommended above. And please let me know how you are doing. Good luck.

QUESTIONS FOR EXECUTIVES ON CYBER

During my career (Amoroso), it's been my honor to have served alongside some of the most capable and talented corporate executives in the world. One such executive, Andy Geisse, now serves as Operating Partner at Bessemer Venture Partners, after having served as CEO of AT&T's massive $71B business services unit. (Yes, that is a seventy-one.) Andy and I have kept in touch since our departures from AT&T, and we've recently been going back-and-forth on something that I think you'll find interesting.

What we've been doing involves creating cyber security-related questions that board members can ask management teams, and that management teams can ask operational groups. We agreed that the questions must be direct and simple, but that they must also be substantive enough to stimulate useful discussion. Our select categories focused on typical board and senior management responsibilities, which led us to the following six areas: Risk, compliance, technology, architecture, innovation, and personnel.

One nuance in our discussion was our sincere belief that slightly different questions would be suitable for corporate board members and senior management teams to use.

One nuance in our discussion was our sincere belief that slightly different questions would be suitable for corporate board members and senior management teams to use. Obviously, both entities share the goal of ensuring proper security governance and execution, but senior managers should be probing slightly deeper than board directors – and this is hopefully evident in our questions below. We tried hard to trim things down, and ultimately arrived at ten questions for boards to ask, and twenty for senior management.

Below are the questions we agreed upon, along with a brief recommendation on how the interrogator might go about interpreting answers received. Hopefully, such commentary will be unnecessary, since our questions include no buzzwords, nothing particularly complex, and only straight talk about common-sense issues. We hope that you will forward this article to any board members or executives in your orbit, and that they will cut-and-paste these questions into the agenda for their next cyber-related review.

---------- clip here and send to your Board of Directors ----------

BOARD QUESTION 1 (RISK): What are the greatest risk areas to our organization from the perspective of cyber security, and how are they categorized? *(The answer should not be vague but should instead clearly and directly connect cyber risk to business objectives and goals.)*

BOARD QUESTION 2 (RISK): What are the major functional, procedural, policy, and governance means by which we mitigate these identified cyber risks? *(This answer should include sufficient detail to demonstrate a good working knowledge of the mitigation methods.)*

BOARD QUESTION 3 (RISK): What is the recommended method for the Board to measure and monitor cyber risk? *(This can be answered by explaining possible frameworks and even commercial platforms that can establish a meaningful metric.)*

BOARD QUESTION 4 (RISK): Have we seen specific, directed cyber threats against our organization, and do we believe we have any known adversaries? *(The response here can include specifically-named adversaries, or might just include a broad survey.)*

BOARD QUESTION 5 (RISK): How will we respond to serious cyber incidents that might negatively affect our customers or brand? *(The organization should have predefined incident response procedures, including public relations statements that have been pre-vetted before an incident occurs.)*

BOARD QUESTION 6 (COMPLIANCE): What security frameworks do we use when audited, and how do we stack up against the requirements? *(This should not be a formal answer with detailed mappings, but rather a general answer of how well the organization does with framework requirements.)*

BOARD QUESTION 7 (COMPLIANCE): What specific audits have we been subjected to, both internal and external, and how are we doing in such audits? *(This is a question that is rarely asked, and many specific external security audits, often by large customers, are performed without reports to the board or senior management).*

BOARD QUESTION 8 (COMPLIANCE): What overall cyber security solutions and risk reduction measures should be deployed that are not currently in place? *(The board should not assume that compliance frameworks will achieve this objective, even if the answer is a return to basics.)*

BOARD QUESTION 9 (INNOVATION): Do we stack up well against our competitors in cyber security? *(This should be answered with evidence that the organization is within reasonable bounds of how other organizations address cyber security. Most companies invest roughly 5% of the IT budget for cyber, for example.)*

BOARD QUESTION 10 (PERSONNEL): Do we have the right team in place for cyber security? *(This question should be answered carefully, with attention to the tenure of the current Chief Information Security Officer. High turnover on the security team is a bad sign.)*

---------- clip here and send to your Management Team ----------

MANAGEMENT QUESTION 1 (COMPLIANCE): Which security compliance frameworks do we address in our company? *(The answer should be crisp and should highlight relevant frameworks such as the NIST 800-53 or the Payment Card Industry (PCI) Data Security Standard (DSS).)*

MANAGEMENT QUESTION 2 (COMPLIANCE): Do our auditors understand our security infrastructure and are they addressing the right issues? *(The answer should include input from both the internal and external auditors, as well as the lead information security executive.)*

MANAGEMENT QUESTION 3 (COMPLIANCE): What governance, risk, and compliance (GRC) processes and automation do we use? *(The answer should reference use of a specific GRC platform and associated methodology for automating, managing, and tracking risk.)*

MANAGEMENT QUESTION 4 (COMPLIANCE): What are the one or two key compliance metrics worth tracking? *(The answer should be consistent with metrics presented to the board and should not be complex or difficult to interpret. Number of actionable insights per year is an example.)*

MANAGEMENT QUESTION 5 (TECHNOLOGY): How do we canvass, review, and select the most appropriate security technologies? *(The answer is that a source selection process for vendors and technologies should be in place with proper criteria for product and service procurement.)*

MANAGEMENT QUESTION 6 (TECHNOLOGY): Which security technologies are currently working well, and which are not? *(The answer is that certain technologies such as real-time attack detection and anti-virus software might be considered suspect, whereas others might be more effective.)*

MANAGEMENT QUESTION 7 (TECHNOLOGY): What security technologies will be important to our organization in the next five years? *(The answer should identify a few technologies that can be clearly connected to the objectives of the business in the coming years.)*

MANAGEMENT QUESTION 8 (TECHNOLOGY): If we had an unlimited budget, what technologies would we buy that we do not currently have? *(The answer should be clearly stated, perhaps focusing on artificial intelligence, contextual authentication, or other emerging technologies.)*

MANAGEMENT QUESTION 9 (ARCHITECTURE): Can our current security architecture be described in simple terms? *(The answer here is not an easy one, so expect some difficulty in providing an answer. There should, however, be some basis for the security set-up.)*

MANAGEMENT QUESTION 10 (ARCHITECTURE): Who is responsible for security architecture planning and design? *(The answer should be clear and should not include too much distributed responsibility. Operations can be distributed, but planning and design should be centrally coordinated.)*

MANAGEMENT QUESTION 11 (ARCHITECTURE): What are we doing to address enterprise security perimeter weaknesses? *(The answer should point to an evolution to a perimeter-less architecture using cloud, mobility, and virtualization to reduce risk of firewall leakage.)*

MANAGEMENT QUESTION 12 (ARCHITECTURE): How will cloud and mobility technologies factor into our evolving security architecture? *(The answer should be that cloud and mobility are central in the protection of data for internal and third-party usage.)*

MANAGEMENT QUESTION 13 (INNOVATION): Have we implemented any innovative new protections in recent years? *(The answer should include at least some modern cyber protections based on recent innovation such as machine-learning security.)*

MANAGEMENT QUESTION 14 (INNOVATION): What security-related intellectual property and patents do we currently hold rights to? *(The answer should clearly define the IP and patents the organization might have rights to, or own.)*

MANAGEMENT QUESTION 15 (INNOVATION): What process do we follow for performing security research and development? *(The answer should address how the organization performs or takes advantage of world-class research and development in cyber security.)*

MANAGEMENT QUESTION 16 (INNOVATION): How do we encourage and support security innovation in the company? *(The answer should describe how employees and third parties are encouraged to innovate to improve cyber security.)*

MANAGEMENT QUESTION 17 (PERSONNEL): Can you provide evidence that our information security team is world-class? *(The answer to this question should include clear evidence of team competence including past performance, experience, and expertise.)*

MANAGEMENT QUESTION 18 (PERSONNEL): Are we paying good salaries and offering a desirable environment for the security team? *(The answer to this question should include benchmark data showing how salaries match up with industry. Retention metrics would be useful in the answer as well.)*

MANAGEMENT QUESTION 19 (PERSONNEL): How do we recruit fresh blood and new talent to the security team? *(The answer to this question should include clear evidence of how team members are recruited, including any university programs.)*

MANAGEMENT QUESTION 20 (PERSONNEL): Do we nurture our external reputation and interaction with the security community? *(The answer to this question should address how the security team interacts with the standards community, conferences, and forums.)*

WHAT FOUR WOMEN CYBER SECURITY EXECUTIVES SAY ABOUT LEADERSHIP

Since joining TAG Cyber in September 2019 as a senior analyst, I've taken—along with Ed—more than 350 vendor briefings. Three hundred and fifty might actually be a conservative estimate; as the only two analysts in our small startup, we've only recently begun to track numbers of calls and meetings. But whether it's been 250 or 500, it's a lot of conversations with cyber security product and service companies, day in, day out.

Still, those briefings are just a fraction of the cyber vendor market. The vendor directory on the TAG Cyber website includes just north of 1,700 companies, and the directory is far from complete. As I have listened to companies' stories and product presentations, I've come to know a good number of smart, savvy women leading their organizations. Still, I started to wonder how much of this is a self-fulfilling prophecy. As a lesser-known player in the IT analyst space, I reach out to more vendor companies to schedule briefings than vice versa. That in and of itself is a break from tradition. Therefore, I started to wonder if I was subconsciously biasing myself toward women-led organizations or if my perception of the market was skewed based on a bit of self-selection. Fortunately (unlike for call counts), we have loads of data at TAG Cyber so I started some digging.

GENDER IMBALANCE

As a woman in security, it's hard not to notice the gender imbalance. I've written about the lack of women in cyber before, and when I was running content for a cyber security events company, I tried my hardest to boost non-male speaker representation. When I last published on the topic of women in cyber, the industry could only claim 11% representation. More recently, however, studies put the number of women working in cyber security at between 20%[1] and 25%[2].

There's some good news! But it did make me wonder about women in leadership positions at cyber security vendor companies, specifically, women CEOs. Thus, our team spent a few weeks sorting through our vendor database and CRM to see what percentage of security companies are currently led by women. It turns out, that number is 5.07%.

These issues, combined, make it harder for a woman to pursue or want to pursue a highly-visible leadership position where criticism is rampant and when certain actions displayed by a woman might be described as "bossy" (or worse).

This felt like a let-down after seeing the representative percentage of women in cyber grow so rapidly over the last 3 years. After a little more research, I learned that 5.07% is a tad low compared to the percentage of women CEOs among the Fortune 500[3] (6.6% as of June 1, 2019) and the S&P 500[4] (5.8% as of May 1, 2020) companies. Thus, there's a little catching up to do.

But only if we're content to stay on trend with cross-industry statistics. And security doesn't seem to me like the right industry to work in if you're OK with the status quo.

If a double-digit increase in the total number of women working in cyber security can be achieved in only a few years, what's stopping women from assuming more CEO positions? I turned to a few of the impressive women cyber security leaders I've spoken to over the last eight months to learn their take. They are (in alphabetical order): Debbie Gordon, CEO of Cloud Range, Dana Tamir, VP Market Strategy of Silverfort, Ellison Anne Williams, CEO of Enveil, and Natali Tshuva, CEO of Sternum.[5]

IT IS WHAT IT IS…FOR NOW

To start, I asked the executives why they think the number of women CEOs is so low, and, unsurprisingly, everyone agreed that the number is a direct reflection of our male-dominated industry. "Few women get into security to begin with, let alone stay in the field long enough to rise to leadership positions or start their own company," responded Tshuva, noting that her start in cyber was a result of her experience in the Israel Defense Forces' elite 8200 Unit where she was one of only three women in a division of ~70.

Williams had similar beginnings; as a PhD mathematician who spent the first decade of her career in the U.S. Intelligence community she said she is "certainly familiar with being the only female in the room" and has "been labeled and mischaracterized repeatedly—as has likely been the experience of most women working in tech."

These issues, combined, make it harder for a woman to pursue or want to pursue a highly-visible leadership position where criticism is rampant and when certain actions displayed by a woman might be described as "bossy" (or worse), yet the same actions by a man would be described as "tough," "strong," or "assertive." Gordon, too, acknowledged the challenges of being a female in a male-dominated field but said her approach is to disregard gender differences and instead put her effort into being the best leader she can be. "I don't focus on the fact that I am a female leader," she said, "and I try to inspire others to approach their role in the same way."

INCREASING SUPPORT AND VISIBILITY

Without a doubt, it takes courage and support to climb the ranks in any company, much less in a male-dominated field. Tshuva, Williams, and Tamir all noted that the lower numbers of women in cyber means there are fewer women executive role models, yet all three credit mentors for a part in their success. The group's sentiment is nicely expressed by Williams who said, "Regardless of the statistics, mentorship is key. I've been fortunate to have great mentors—male and female—throughout my career who have contributed toward my current role as a founder and CEO. There is power in having an effective support network and I advocate for making mentorship the rule rather than the exception. Having access to women already working and leading in their chosen field can give future CEOs the confidence to pursue these opportunities." All of the women interviewed for this article stated their strong desire to remain mentors for other women in the field.

In keeping with the idea of mentorship, Tshuva adds, "If we want more women in cyber security, the field needs to actively embrace them and not leave it up to chance," meaning, in addition to mentorship, the field must continue to highlight women in cyber doing excellent work and build better support

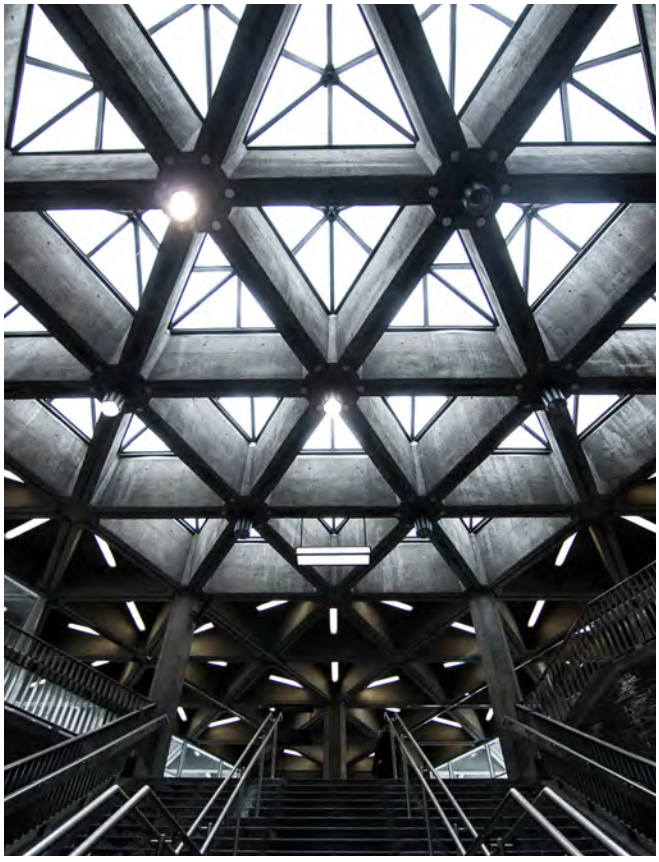
networks of women and men. Importantly, though, it's not enough to showcase women because they are women; cyber security has enough women (percentages not withstanding) doing amazing things—building companies and products, researching ways to fight cyber insecurity, and advising enterprises on strategy after having spent years in the trenches—that every conversation shouldn't be about being a woman in cyber. Instead, the conversation must be about skills, talent, and accomplishments. It just so happens that the people behind the accomplishments are women.

SOCIETAL EXPECTATIONS HAVE A WAY TO GO

Still, Tamir noted that the problem of getting ahead in a field with low female representation can be compounded by culture: "Society is slowly changing, but we still expect mothers to be most heavily involved in their children's lives. Some employers assume that a mother will be less committed [to her job] because she will prioritize her family. [They assume] She will probably work fewer hours or won't be able to pitch in like a man— so they give women fewer responsibilities and opportunities."

Tamir also noted a bit of self-selection when it comes to the grit required to take on a CEO role. "Women tend to self-criticize more than men," she said, citing many studies on how women—on the whole—have a greater tendency to only apply for jobs when they meet 100% of the criteria. Men, on the other hand, apply for positions if they meet just 60% of the requirements.[6]

These barriers, too, can be overcome through strong support networks, both inside the industry and at our academic institutions. There is no pre-ordained industry in which men, women, or non-binary people are more successful based on ability. While the number of women and non-binary CEOs in security are low, the key to attaining a better balance is acknowledgement and acceptance that anyone, from any background, can be successful with training, support, and experience. Whether the goal is to become a forensic analyst or a CEO, success should not be based on anything other than smarts, hard work, and commitment.



"There is a great misconception in cyber that you need a STEM background," noted Gordon. Reality is, though, "that cyber security is about critical thinking—especially a CEO role! You don't need to be highly technical to be a successful cyber CEO, but you do need leadership skills and the ability to identify market opportunity." Anyone can gain leadership skills through a variety of avenues—formal education, books, role-specific training, mentors, and more. Women need to realize that the opportunity is there for the taking, and that can happen with increased support and encouragement.

TAKING THE RISKS

Nonetheless, there are tangible challenges even when a strong woman decides to pursue her dream of becoming a CEO. Tshuva pointed to the numbers; most venture capital is given to men[7], and cyber security is a start-up and acquisition culture. Thus, a woman who wants to lead a cyber security company is up against higher hurdles in fund raising. "Starting a new venture is risky," noted Tamir, and when the odds of equal treatment are stacked against women, the decision to move forward can be discouraging.

Williams agrees that there are risks but says she was able to achieve her position as CEO by "staying focused on the work I am passionate about and where I am confident I can make a substantial difference." She advises that women "can't blaze a trail without first planting the flag through the substance of your own accomplishments."

There is more work to be done to help women in cyber security become CEOs, founders, and achieving other C-level positions. While the current number of CEOs is low, it is encouraging to see the overall population of female cyber security practitioners increasing rapidly, and it's important to remember that, as recently as 1995, there wasn't a single female CEO on the Fortune 500 list.[8]

To grow female representation among cyber security C-levels, it will take a little moxie and a lot of hard work, dedication, and support by the entire security community. Breaking the glass ceiling isn't easy, but we already have many amazing examples, noted above and even more broadly in the field, showing that the opportunity exists for women who want to take on the challenge, can block out any unhelpful noise and disregard all preconceived notions, and focus on learning, listening, and pursuing exciting opportunities without hesitation.

References

[1] https://securityintelligence.com/articles/lets-recruit-and-retain-more-women-in-the-cybersecurity-industry/

[2] https://www.securitymagazine.com/articles/90071-women-represent-24-percent-of-cybersecurity-workforce-isc-reports

[3] https://fortune.com/2019/05/16/fortune-500-female-ceos/

[4] https://www.catalyst.org/research/women-ceos-of-the-sp-500/

[5] N.B. 50% of the women interviewed for this article are CEOs of Israeli cyber security startups.

[6] https://www.bi.team/blogs/women-only-apply-for-jobs-when-100-qualified-fact-or-fake-news/

[7] https://www.marketwatch.com/story/venture-capitalists-still-give-most-of-their-money-to-white-men-study-finds-2019-02-13

[8] The late Katherine Graham, of The Washington Post Co., was the first female CEO to make the Fortune 500 list, in 1972.

PROTECT EMPLOYEES' MOBILE LIVES; PROTECT YOUR ENTERPRISE

Diane is out walking with Harry: *"Harry, what time is it?"* Harry takes his phone out of his pocket: *"It's 3:27 pm."*

Jordan and Jamie are watching football. Jamie says to Jordan, "*Hey, let's order some food!"* Jordan opens one of the many food ordering apps on their phone and asks, *"What should we get?"*

Nate and Ally are leaving to go on their honeymoon tomorrow. Ally says to Nate: *"Don't forget to order a Lyft for 11:00 AM!"* Nate quickly opens his app, orders the pickup, and continues packing for the beach.

Liam is out shopping for a lamp for his new apartment when he spies a couch that would look perfect in his pad. But it's so expensive, and he was only looking for a lamp… He pulls out his phone, clicks on his banking app, is reminded that he's been diligently saving, and buys the couch.

A vulnerability in one of these apps could lead to a data breach, malware infection, or the ability for attackers to gain remote control over parts of our lives—not just our phone.

Eric is at the grocery store and he can't remember if he has enough butter to bake cookies for his roommate's birthday. He takes out his phone, connects to his smart fridge app, and gets his answer, allowing him to leave the store with all the ingredients he needs.

These snippets demonstrate just how dependent our lives are on our mobile phones. For many of us, losing our phone, the data on it, or access to any number of apps would be a severe disruption, nearly catastrophic for some. A vulnerability in one of these apps could lead to a data breach, malware infection, or the ability for attackers to gain remote control over parts of our lives—not just our phone. In a recent finding, security researchers discovered a flaw in a smart tracker that could allow "anyone with basic hacking skills" to track the wearer, listen to their audio, make calls from the wearer's phone, access the camera, or trigger phony alerts.i

Needless to say, the security of our mobile phones is critically important, yet it's an area most consumers ignore. Enterprise security teams, of course, are more cognizant of the dangers and, in fact, have been worried about BYOD and personally-owned phones in the enterprise for as long as personally-owned phones have been in the enterprise. Today, unlike ten years ago, the problem is even more pressing because, 1. most employees' phones are personally-owned and dual-use, i.e., they're used for personal and professional reasons without any isolation between resources, and 2. the app ecosystem is out of control.

While some enterprise security professionals might consider the nature of employees' dependency on their mobile phones a security problem that needs to be fixed, it is, in fact, an opportunity to further the message of security. What I mean by this is, if employees are bringing personal phones into the enterprise, those phones should have an extra level of on-device security. Yes, from the corporate

perspective this means better internal security, which is obviously the charge of the security team. However, there is another aspect to consider: making champions out of employees by highlighting just how imperative personal mobile phone security and data privacy are to the employees themselves.

The reality is, today, most businesses don't provide employees with smartphones because employees generally prefer to use their device of choice, and because it is less costly for businesses to buy every employee a corporate-owned device. While riding the tide of the personal phone means somewhat less control over the device, security teams can implement endpoint and mobile security solutions that isolate environments, check device integrity, scan for vulnerabilities and malware, and much more. In fact, the market has never been more ripe for endpoint and device security.

Thus, from a company perspective, there is plenty of security that can be forced upon employees. In many cases, this system works from a control perspective, but any security team recognizes that employees will find ways around corporate security when they can. And when it comes to their personal mobile devices—even if work-related apps and tasks are part of usage—employees will be creative, bobbing and weaving around controls if they can't do what they want to do on their phones. After all, some manufacturers are pushing the idea that their devices ship with the highest-level security. It's become a mainstream marketing message and a competitive differentiator.

But security practitioners know he state in which a device ships isn't the only consideration. It's how employees use the phones they have, what they access, what they download, with whom they share content. This is why it's far better for corporate security teams to focus on the personal benefit of the employee/consumer/individual when implementing security controls rather than on the message: *You need X controls deployed on your phone to use corporate resources. If you don't do Y this way, you can't access Z.*

In this light, mobile security becomes: *this is your life you're protecting!* Of course, enterprises don't have to ask permission to deploy mobile security controls to endpoints touching corporate resources. Mobile device and endpoint security companies aren't having any trouble gaining traction amongst enterprise security teams. Yet, when it comes to acceptance and championing security initiatives, it helps to build a fabric around what matters to people so that enforcing security isn't always a fight between control and end user needs/wants/preferences.

With work from home elevating mobile security, the fact that some employees are being forced to use their personal devices as work devices, and recent hacks like the one targeting dementia patients driving home the personal nature of attacks against personal devices, now is a good time to push mobile projects forward.

Even though it might be easier now than ever to secure funding for a mobile initiative based on enterprise need, it would be advantageous to evangelize a message that employees—individuals—can buy into and help propagate based on their desire to improve their own lives

Imagine this future conversation rather than the ones you're having now:

Non-security employee: *"Hi, security person. I just read about this cyber attack on my food ordering/ fitness/ride sharing app and a bunch of people had their data stolen. Do we have anything like that at work that could help with that?"*

Security employee: *"Why, yes! It's called Lookout. I can install it."*

[A minute or so later] Non-security employee: *"Cool, when?"*

Security employee: *"Done."* (Said as security employee scans employee's apps for malware.)

LAW FIRMS CONSIDER THE VIRTUAL CISO

Law firms have come late to the cyber security party. It took attacks on well-known firms—especially the one on DLA Piper, which completely shut down all telephones and email of one of the world's largest firms for two full days--to wake them up.

Are they now the cyber security equivalent of "woke"? They're getting there. But some surveys suggest they still have a ways to go. A third don't have standalone cyber insurance policies. Only half have designated cyber security teams. And a fifth don't have a data breach plan in place. Even though, according to an American Bar Association survey, 25 percent have suffered a data breach at some point.

Law firms are beginning to recognize that they are vulnerable to cyber attacks. Yet a third still don't have standalone cyber insurance and half don't have cyber security teams.

The law firms that are in the best shape are probably the largest ones, which have the most resources. Small- and medium-size firms seem to be lagging. And one area in which they can use help is in their staffing.

Most of the large firms have chief information security officers (CISOs). But plenty of the smaller ones don't. And it's not hard to understand why. CISOs are in great demand and short supply these days, and they can command salaries of $200,000 and up. That's probably out of reach for lots of smaller firms.

Yet, this is a particularly important time to have a CISO. The Covid-19 pandemic has forced law firms to ask their attorneys to work from home for months. And this new arrangement has added risks that

have prompted some firms to create new policies that may require training and monitoring. A CISO's leadership in this area would seem to be desirable if not essential.

For firms that have not yet hired a CISO, there's another solution. They can hire a virtual chief information security officer, or vCISO.

Let's make one thing clear from the start. The word "virtual" here does not mean that a vCISO is the equivalent of Siri. It means that the CISO works part-time.

There are several reasons law firms may want to opt for one. Some firms are not quite ready to make the leap. They may be loath to pay a fulltime salary and benefits. And they may only need someone once or twice a week. The vCISO can report to the office or (most likely under current conditions) work remotely.

Sometimes firms don't feel that they can find one person to meet the disparate needs a CISO may be asked to address. For example, one month a firm may want someone who can do penetration testing. Another month it may want audit testing to help it prepare to pass an audit. One person may be able to handle both, but it may be easier and faster to swap in people for each project.

What law firms need to attend to first and foremost, of course, is client data. One of the first things DLA Piper said when the firm had recovered its ability to communicate with the world, was that it didn't think any client data had been lost or compromised.

Other firms have not been so lucky. Some of the biggest law firm breaches, like the Panama Papers scandal, have demonstrated that one attack can destroy not just a firm's reputation, but also its business. That has undoubtedly opened the eyes of the industry. As have the growing number of ransomware attacks.

A particularly nasty variety surfaced recently called a Maze attack. Not only is a law firm's data encrypted, but some data is stolen and held hostage. If the firm doesn't pay quickly, the attackers slowly make the stolen data public. It's one more reason why companies that possess valuable data would be well advised to employ skilled and experienced security professionals.

And now that so many lawyers are already working remotely, this could be a good time to try a virtual CISO. By not being there, they will fit right in.


INDUSTRY

IT'S TIME TO BREAK UP THE RSA CONFERENCE

In 1983, the late Harold Greene presided over a consent decree that broke up the Bell System. While you might debate the national security implications of that divestiture, you cannot debate the innovations that followed. Just a quarter century later, for example, we all watched as Steve Jobs hopped on stage to demonstrate the new iPhone. I believe this superb invention, and many other advances since, were enabled by the break-up.

Which brings me to the RSA Conference. I first started attending the annual event in the mid-1990's, and believe it or not, the conference during that period was both relevant and edgy. It made real news, held real fights (remember Clipper), and accepted real technical papers by real experts. I still have one of those iconic RSA Conference posters from the mid-90's showing NSA as the only agency that "listens to its customers." *Awesome*.

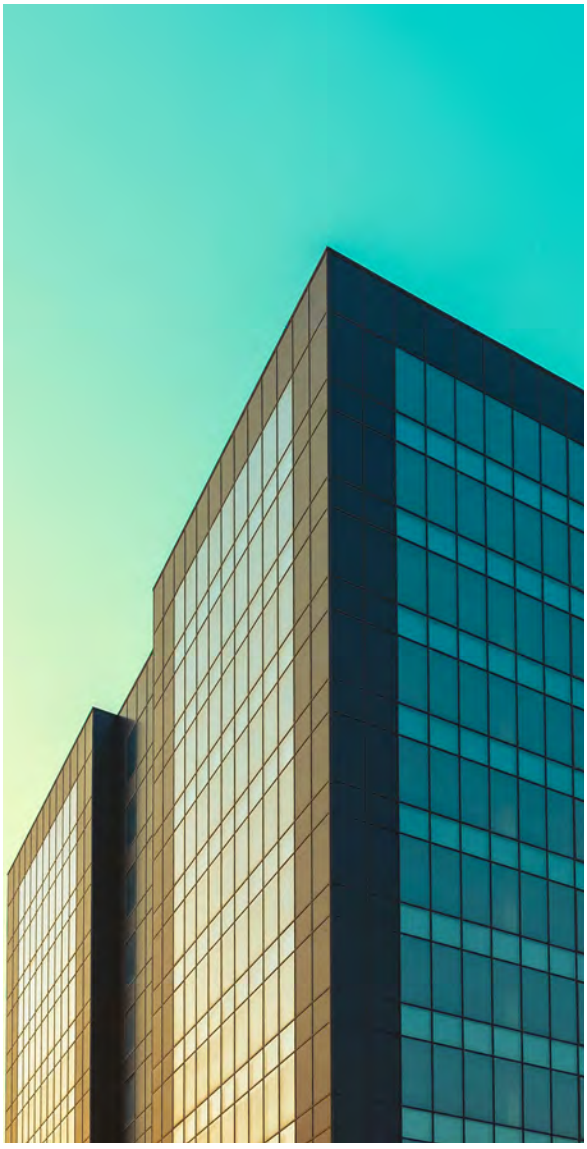
Today, however, the RSA Conference has devolved into a routine event for mid-lifers with booth-after-booth-after-booth of the same-old, same-old. And just as with AT&T in 1983, this situation was not caused by bad leadership, but rather by that terribly unavoidable corporate condition: The dreaded S-curve. I believe the RSA Conference has finally reached the top part of that scary curve, which is why it's time to take action.

Let me acknowledge that the RSAC corporate ownership, its fine program committee, and its expert conference advisory board will explain that they've evolved the event. They will point to the new programs, sessions, competitions, and on and on. But look – AT&T said all the same things back in 1983. They were just as averse to change as I suspect RSA leadership will be to my recommendation. No one likes change, really.

But not acting will be bad for business. Steve Martin, for example, quit his stand-up act back in the 70s when he noticed just a couple of new empty seats in the back row. Similarly, I'd recommend that RSAC leadership act accordingly while the conference is still strong. If they don't take action now, then RSAC will continue its slide toward becoming the cyber security equivalent of (ahem) a Wayne Newton Show in Vegas.

Here's what I recommend: RSAC leadership should sunset the existing advisory board (no offense to my friends). It

The RSA Conference has devolved into a routine event for mid-lifers with booth-after-booth-after-booth of the same-old, same-old.



should then create five new program committees with no member over twenty-nine and at least two-thirds women. These five new committees should then caucus over beers outside Whisler's to reinvent five crazy-interesting conferences with themes that are meaningful and edgy. They should push the envelope.

Then the PCs should reinvent how these five new S-curves are physically held. It could be something cool like those crowdsourced, simulcast, conference-BNB things. Maybe it could involve using the headquarters of security companies from around the world. Instead of having physical booths at Moscone, vendors could host concurrent RSAC three-day parties for anyone who chooses to come to their venue. Or whatever. It would be fun.

Look – I know this would be a jolt, but if RSAC continues on its present path, then here is my prediction: Within three years, the RSA Conference will book less than 20K paid attendees, and it will start to lose its grip on the vendor community. Perhaps worse, the current show is really turning into a BoomerCon. Just like Spot the Fed at DEFCON, RSAC could initiate a Spot the Non-Boomer contest. It would be quite a challenge.

By the way, Black Hat is the new RSA Conference. Just look at this sponsorship page for a conference that started as anti-establishment. Rich Powell and I developed a cartoon to lampoon this inevitable transition. You see, Black Hat is riding up the middle of its S-Curve. It is still somewhat edgy, and still somewhat relevant. In a few years, I'll probably be whining that they please stop kicking their conference can down the road.

Oh – and there's this: RSAC 2020 attendance looked to our TAG Cyber team to be about 50% down. This had nothing to do with the conference and everything to do with the virus. But it is precisely such random events that can trigger a downfall. Some security vendor or enterprise team might notice, for example, that the earth continues to rotate despite not having been at RSAC. This leads to a decision next year to maybe . . . well, you get the idea.

I believe that breaking up RSAC into five new conferences is good business for the owners and healthy for our industry. Even the venerable AT&T, where I spent most of my adult life, thrived mightily post-divestiture despite decades of fighting the courts. If RSAC ownership wants to protect its investment, then they will listen to my advice. If they don't – well, at least RSAC 2025 will be easier to navigate, because no one will be there.

I hope they listen.

CONFERENCE BOOTHONOMICS

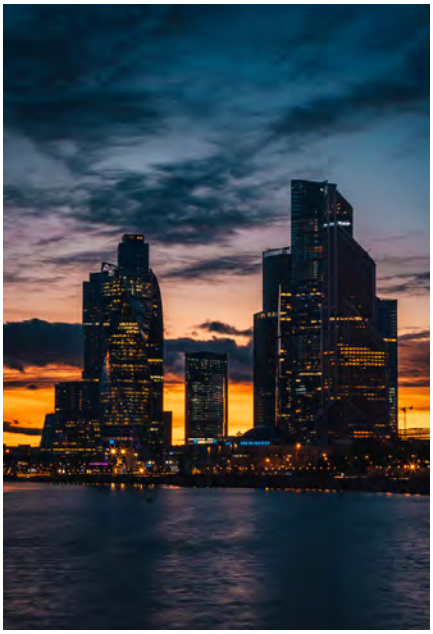
This article was written a year before the COVID-19 crisis arrived. It's interesting to read now the guidance offered on conference booth management. It's also interesting to see that the last word of the article – written long before social distancing and masks, references our worst nightmare in any modern interaction between strangers: Spit.

"Excuse me, ma'am . . . might I interest you in our cloud-based, mobility-enabled, threat-intelligence powered, machine-learning security solution? . . . uh, why don't I first scan your badge . . . hmmm, why isn't this working? . . . oh, good – there we go, now I have it . . . uh, did I tell you that we shrink the attack surface while rendering your adversary useless without the need for complicated agents or signatures?"

When attendees see hopscotch, Nerf basketball, or other boothbarker-led gimmicks, then they conclude that you are bored with your own solution – and this can be infectious.

With the RSA Conference at T-minus two weeks, I wanted to share some heartfelt advice with those of you now doing vendor booth planning. My advice comes from many years of standing on either side (seller and buyer) of that little porto-table with its stacks of data sheets and bowls of Hershey kisses. My hope is that this advice will help you to maximize the ROI for your little slice of exhibitor heaven in Booth 7002 of the South Expo.

KNOWLEDGEABLE STAFF – The first axiom in security conference boothonomics is that the best people in your company should be covering the floor. When you use greener-than-Kermit sales engineers to staff your booth, you basically shout out that you don't value the engagement. Look, if you're a CTO or CEO, then ask yourself: During the day-and-a-half of booth-time at conferences like RSA, do I really have something more important going on?



On the other hand, when you staff the booth with knowledgeable principals who can speak with confidence and authority, then you are telling attendees that you appreciate their decision to pause for a chat. And if you cannot deal with this first requirement, then dare I say that it would probably be better to skip the conference entirely. Stated simply: Bad support with thin staff is worse than no booth at all. (Gulp).

AVOIDANCE OF HYPERBOLE – A second axiom of boothonomics for security is that the most powerful claims are based on facts, without nonsensical hyperbole. When the boothmeister starts shouting that their platform does security better than everyone else, and that they can deal with absolutely 100% of every cyber security threat that anyone could ever imagine, well, then you are in the hyperbole zone, and it's time to move along to the next vendor.

My advice: Coach your team to be calm, reasonable, and understated in all discussions. They should listen carefully to

attendees, perhaps taking notes on the conversation. And your team should avoid the temptation to talk faster with big words and passing more spit than should ever be allowed in a public place. Hang a little sign on the back of your booth table that reminds your team to do this: Listen. Do Not Exaggerate. Be Understated.

NON-GIMMICK ZONE – The third axiom of security conference boothonomics is one that mercifully and thankfully ended those ridiculous Booth Babes of the Evil 90s. The axiom states that gimmicks do not work in booths (or in life), and that if you need circus games to attract visitors to your conference display, then you should seriously rethink your overall security product or service methodology.

When attendees see hopscotch, Nerf basketball, or other boothbarker-led gimmicks, then they conclude that you are bored with your own solution – and this can be infectious. So, please avoid the gimmicks at your booth, especially because they inflate that dreaded booth-traffic metric – which relates to boothonomics, as clicks and views relate to flashy web start-ups. Neither generate any revenue. (Deals generate revenue).

And now – a word to attendees: I know that enterprise security is a helluva-tough job, and that your life is one hack away from headhunter hell. But please show some respect for those men and women working the vendor booths. They are as aware of the ridiculousness of this dance as you are, so show some mercy . . . unless, of course, they start talking fast and spitting in your face about their best-in-class AI. Then you can roll your eyes and move on.

I hope you all enjoy San Francisco in March, and please share with me any new security vendors you discover in the Exhibit Hall that you'd like me to cover in an upcoming column. I'll do my best to get something written (without hyperbole . . . or spit).

AN HONEST TEMPLATE FOR GDPR PRIVACY NOTICES

Dear Customer:

The General Data Protection Regulation (GDPR) has now been active for <insert duration since May 25, 2018>. As your Data Processor, we are writing to you because we accidentally noticed that <insert name of your top competitor> has already been doing so. Our newly appointed GDPR Data Protection Officer, <insert name of your lowliest office clerk>, has developed the following list of privacy promises, after a Google search:

1. If we think that we are doing a bad job of <insert how you process data>, then we promise to quickly revise our opinion of what we do.

2. If you would like to send us a security questionnaire, then we promise to forward your email to <insert name of your phishing abuse desk>.

3. If we protect your data with <insert firewalls, anti-virus, or passwords>, then please relax, because our lawyers said these will hold up just fine for us in court.

4. If our staff is authorized to read your data, then we promise to make them recite <insert your company oath> to ensure their full loyalty.

5. If you choose to exercise your Data Subject rights, then <insert name of your lowliest clerk> promises to respond, although we honestly don't know how, or even why.

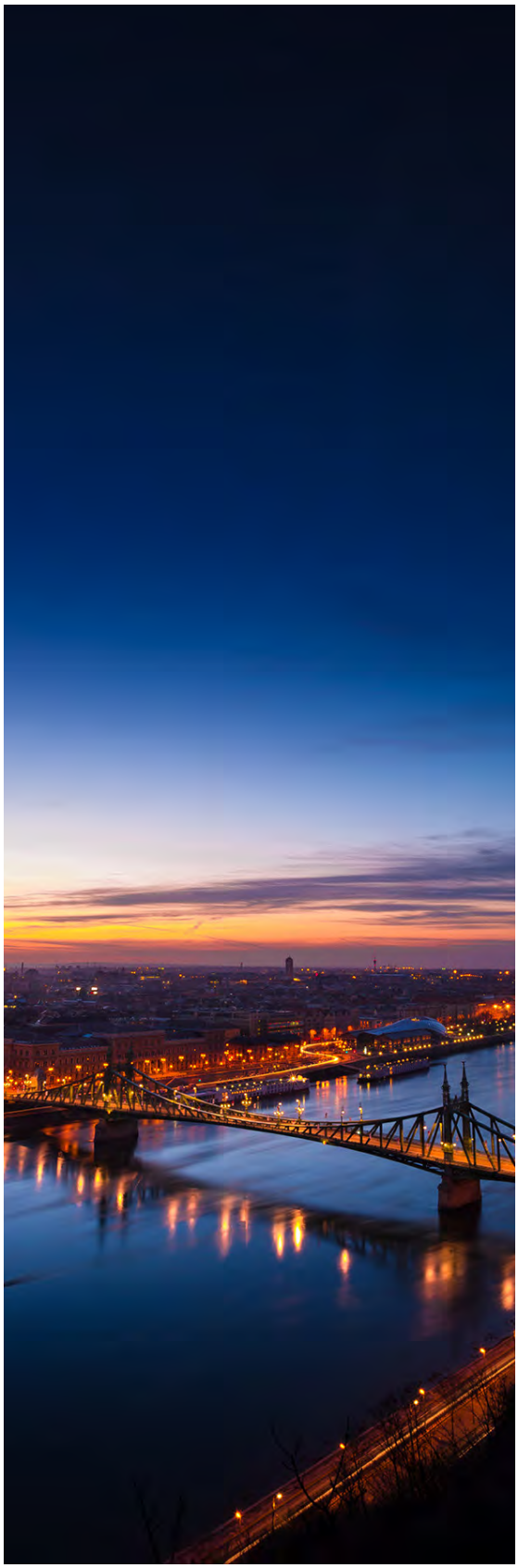
6. If we are using a third-party to <insert how you process data>, then please contact them directly and let us know what they said.

7. If your data is ever compromised by <insert description of data breach>, then we refer to you to bullet 6 just above.

Compliance with <insert 'the' if you are European, else omit> GDPR is of the utmost importance to <insert name of your company>. If you have any privacy-related concerns, or if you would like to thank me for keeping this note to one page, then please contact me at <insert name of your phishing abuse desk>.

Yours in privacy,

<insert name of your lowliest office clerk>



MODERN DATA SECURITY: WORSE THAN YOU THINK

Imagine that under some bizarre set of circumstances, a local high school football team is forced to compete against the New England Patriots. Imagine further that the victory stakes for these teenagers are enormous, perhaps even life or death. Let's complete this nightmare situation with an understanding that the NFL team will not let up one inch. They will play full throttle, no holds-barred, and they will hit – hard.

The CISO has become, in a sense, a local civilian defense commander

If you are the coach, the superintendent, or the mayor – what would you do? Any thoughts of calling this ridiculous mismatch off must be forgotten; the game will be played, and the stakes will be consequential. So, what would you do? How would you address these unfair odds? Sadly, this ridiculous scenario perfectly illustrates the challenge of cyber security teams when dealing with nation-state actors.

This mismatch can be understood by examining the evolution of the corporate information security profession. Just as personnel departments have evolved from typists creating employee badges, information security departments have similarly progressed from technicians putting anti-virus software on PCs.

Unfortunately, while the personnel team has blossomed into a vibrant (and renamed) Human Resources team with its top executive reporting directly to the CEO, most data security teams are stuck, led by a middle-management executive called the Chief Information Security Officer or CISO. The CISO is generally viewed by the CEO as unfit for any other position, and is often fired when a breach occurs.

Most CISO-led teams are staffed and funded to deal with a so-called reasonable adversary. That is, their programs were designed to detect basic hacking, using common tools such as perimeter controls, anti-malware software, and identity systems. Larger programs in banks and telecom firms might super-size these components and introduce fancier tools, but the emphasis is the same: It's one high school team set up to deal with another high school team.

However, in enterprise cyber security, the adversary is no longer just the basic hacker. Instead, the CISO must now craft a new type of program to somehow stop well-trained, professional foreign military attackers from breaching their systems. The CISO has become, in a sense, a local civilian defense commander, tasked with handling cyber backlash when national leaders openly recommend more intense attacks against adversary nations.

Much of the above will not come as a huge surprise. That is, data security breaches have been increasingly common events, and everyone knows that nation-states sponsor a great number of these attacks. But the currently-popular solution of imposing stricter compliance demands is akin to the local superintendent handing the football coach a formal proclamation that the Patriots be defeated – or else.

Compliance programs, such as the European Union's emerging Global Data Protection Regulation (GDPR) certainly have their place. It is reasonable, for example, to demand that users be offered easy-to-read details of business policies put in place by a data handler. Bad privacy policies are unacceptable and regulating their details is reasonable. But compliance requirements do not address cyber security breaches. In fact, they can often make things worse.

Let's return to our high school football analogy: To deal with the upcoming Patriots game, suppose that the superintendent develops compliance controls that the local coach must follow during the game. Auditors will ensure that if these controls are violated, the coach will be personally fined and fired. But in a bizarre twist, the compliance controls will be published for all to see – including the Patriots! Compliance is public; the adversary gets to see your plans.

Overly strict compliance controls with demanding documentation requirements bog down the CISO-led teams into a nightmare of paperwork and administrative processes. Furthermore, they stymie creative cyber defenses, particularly after a compliance project has been completed. Who, for example, would ever recommend network or system adjustments after a network has been certified? The result is a basic paralysis resulting in architectural stagnation.

THE SOLUTION HAS THREE ELEMENTS.

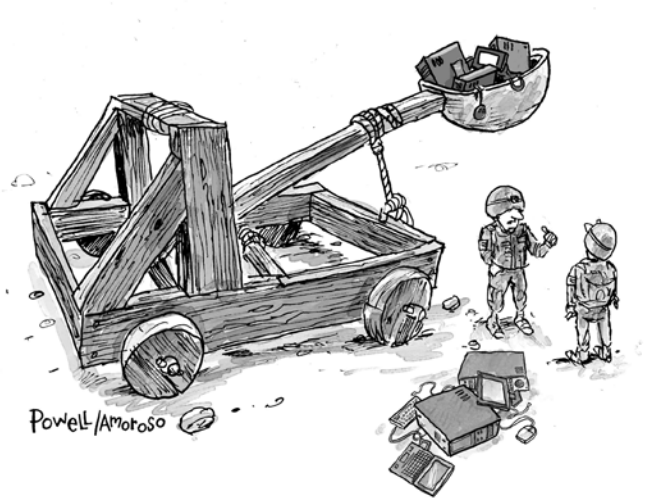
First, we must begin to untangle CISO-led teams from the barrage of compliance requirements they are asked to support. The GDPR, for example, can get in line behind dozens of other controls such as NIST 800-53, PCI-DSS, and HIPAA that are currently bogging down enterprise cyber security teams. Stricter compliance is simply not the answer to data breaches.

Second, enterprise CISOs must be elevated to more senior positions with greater power and leadership. They should be selected based on their ability to run a complex organization, rather than their ability to write rules for an intrusion prevention system. CISOs should be funded as purveyors of civil defense, rather than as the handlers of trivial awareness messaging for sloppy employees. And they should only be fired after a breach if they deserve it.

Third, enterprise leaders must recognize that the entire business enterprise must be completely redesigned, with different policies, systems, and third-party support to stop nation-state attacks. The cloud, for example, should be viewed as helping rather than hurting cyber security. Again, consider your high school coach: To defeat the Patriots, major changes in personnel, practice, and technique would be required. The whole program would need to be overhauled.

By the way, it would be nice to imagine that perhaps negotiating with nation-states might solve this cyber problem. But security experts have observed for years the so-called Roger Bannister effect for cyber attacks. That is, just as the four-minute mile opened the door for others to easily pass that time, nation-state sponsored cyber attacks have opened the door for many others to do the same. They open the flood gates, by example, for less capable hacking teams.

Let's hope that in the coming years, particularly as the GDPR ecosystem begins to levy massive fines on breached companies ill-equipped to deal with the types of threats being directed at them, we will take a moment and reflect: Compliance does not stop data breaches; only revamped cybersecurity programs can do that. And if the CISOs tasked with protecting our data are underserved, then you can be certain that all of us will be underserved as well.



"I don't think our commander quite understands cyber war."

WHY DO-IT-YOURSELF SECURITY IS NOT RECOMMENDED FOR EXPERT SOFTWARE DEVELOPERS AND SOC ANALYSTS

The tendency for software developers and enterprise security operations center (SOC) analysts to create do-it-yourself solutions to protect critical data from cyber threats in cloud environments is not recommended. This note explains the issue and suggests practical commercial alternatives.

INTRODUCTION

The protection of critical data from cyber threats is a problem that is often presumed to reside primarily in the enterprise. With one company after another seeming to fumble their customer data and user credentials, it is not surprising that so much attention has been placed in the cyber security industry on the development of commercial solutions to address these enterprise-oriented problems.

Some organizations might assume that since the major infrastructure providers excel at the security of the environment, their workloads are also protected.

Observers should recognize, however, that malicious threats to critical data exist far beyond the familiar confines of enterprise infrastructure, especially as the use of cloud and containers is on the rise. Software developers engaged in modern CI/CD (continuous integration/continuous delivery) processes, and expert analysts working in security operations centers (SOCs), have similar challenges with data protection, albeit with fewer commercial options to reduce their risk.

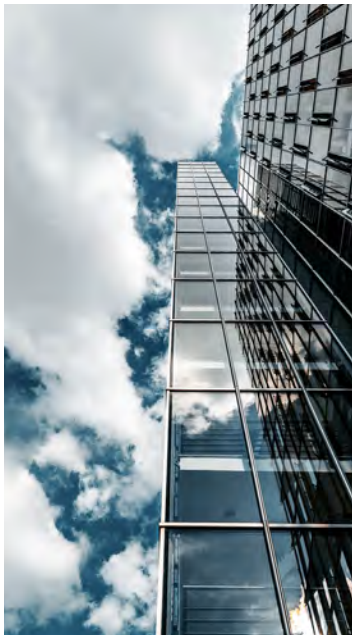
In particular, the security of workloads put in cloud environments by development teams, and the ability to monitor and protect those workloads by SOC teams, are problematic given the limited availability of commercial, end-to-end security platforms. Some organizations might assume that since the major

infrastructure providers excel at the security of the environment, their workloads are also protected. But that is a miscalculation which could lead to unintentional exposure or breach.

This analyst note from TAG Cyber explains the cyber security risk to development and SOC analysis environments and outlines how common attempts to create do-it-yourself security solutions are suboptimal from a risk management perspective. Instead, as this note will demonstrate, these expert practitioners should consider the commercial options now available that will meet their security needs more effectively.

THREATS TO SOFTWARE DEVELOPMENT PROCESSES

Software development is crucial to organizations' abilities to meet customer, employee, and partner requirements. Continuous build/deploy cycles allow developers to meet these demands in a quick, scalable way without the excessive manual oversight of pre-CI/CD lifecycles. CI/CD extends plenty of benefit for building software and applications, and allows developers to make use of faster, less expansive environments like cloud and containers, but several workload security challenges exist.



To start, developers use a number of tools to manage CI/CD pipelines—from pre-commit, to commit, build, test, and deploy, all the way to production. Some of these tools incorporate cyber security functionality, while others lack security governance and integration with third-party security tooling.

Without end-to-end visibility, monitoring, or control, each separate step or integration in the CI/CD pipeline surfaces a vulnerability that attackers can exploit. In other words, in this traditional set up, the strength of the system relies on each component being deployed, configured, and managed individually.

There is also a lack of automation amongst these components, meaning, at each new command line interface, there is a possibility for a breakdown of the pipeline. For instance, if a new application is moving from "test" to "deploy" and a security vulnerability is found, the process breaks, thereby slowing down the cycle. Delays are the nemesis of modern-day development.

Finally, with the myriad tools used throughout the pipeline, it's common for developers to use, reuse, or share credentials. From a security standpoint, this is very risky; if an attacker gets ahold of one set of credentials, it's likely they will be able to find other access at other points and use those credentials to further an attack.

While the individual tools marketplace for security testing—whether SAST (static application security testing), DAST (dynamic application security testing), or source code analysis—is strong, it is optimal for organizations to deploy a unified platform that can see across all stages of the CI/CD pipeline which identifies software-based threats, independent of development environment.

THREATS TO SECURITY OPERATIONS INFRASTRUCTURE

PROLIFERATION OF TOOLS

As with the development environment, SOC analysts are responsible for the management of numerous, and sometimes disparate, IT and security technologies that aid them in detecting, evaluating, investigating, and responding to security events and incidents. Within any one organization, the totality of the infrastructure can look like a patchwork of environments, dashboards, and data streams.

The typical SOC monitors and analyzes each network and the servers, applications, and endpoints communicating on and across infrastructure.

Given the wealth of infrastructure and traffic operational in each environment, the ability to gain uniform visibility and thus establish baselines and identify anomalies can be extremely challenging, because many tools' outputs aren't standardized, and investigating every alert—even every critical alert—is near impossible because of volume. What's more, SOC teams regularly express dissatisfaction with the efficacy of various categories of tools they manage, leading to additional stress and the desire for security tools improvements.

EXPANSION OF CLOUD

As organizations adopt more cloud infrastructure, SOC analysts are feeling pressure to gain the same visibility and control over their cloud environments as they have with internal networks. Because of the nature of cloud, however, SOC teams cannot merely adapt security tooling built for on-premises environments to cloud infrastructure, nor can they necessarily expect all cloud-native tooling to work ubiquitously across all the major cloud provider platforms (thanks to the competitive postures of the providers themselves). Thus, the desire for cross-infrastructure security tooling is high on many analysts' wish lists, and some SOC teams will build their own security to compensate for this capability in the absence or unfamiliarity of commercial tools.

MAKING METRICS MEANINGFUL

As the primary point of information for security efficacy tracking, SOC analysts need technologies that can collect, correlate, combine, and provide actionable data about the environment. To date, security information and event management (SIEM) and aggregated log management systems have been the general weapon of choice for such internal telemetry. However, while SIEMs are excellent at collecting data about network events such as failed login attempts or number of malware handled in a given period, this data does not translate well to business insight and overall risk. Quantity-based metrics don't often translate well to action, meaning, what the organization should do to reduce the number of security events or false positives, or identifying which assets to prioritize in remediation efforts.

As cyber security becomes a top-line business risk, it's not enough to amass data on what's happening in the organization's environments. SOC teams need contextualized data from across their infrastructure to investigate and pass along to business executives, incident response teams, and forensics investigators (when necessary), and they're not likely to get that insight from the SIEM or log management tools. There is an increasing need for technology that can produce data that will allow the organization to act or react to events before they become incidents and demonstrably reduce mean time to detect and respond.

STAFFING PRESSURES

Further, a SOC isn't just an amalgamation of technology; a SOC requires people and processes to run smoothly, and the lack of skilled security staff, as well as insufficient talent pipelines, compound the technology challenges mentioned above. Increased workload can cause burnout among staff, and replacing internal experience introduces gaps in the organization's ability to identify and act upon threats.

CHALLENGES OF DO-IT-YOURSELF SECURITY

OPEN SOURCE

In the absence of, or lack of familiarity with, commercially available cloud security tools, SOC and DevOps practitioners may opt to stitch together do-it-yourself security solutions that are purpose built or obtained from open source options. The good news is that the open source community readily develops freely available tools for all types of security-related problems. Historically, many of the tools provided open source, and based on researchers' desires to improve cyber security, have proven extremely effective.

However, users have to be mindful of what they're getting from open source, as those tools are built by experts and freely provided to the security community for a specific purpose, but then may never be upgraded or further developed. Open source security tools are typically side projects or passion projects, but rarely are they a researcher's or developer's full-time job and thus may not be maintained over time. The consequences include lack of product development or maturation as security requirements move forward. More easily said, open source tools may not adapt as security requirements change, or products may not be updated or patched, when necessary. Open source projects, though they may be developed over long periods of time and out of necessity, are frequently one-and-done, meaning the developer/creator had no intention of further development. This can lead to control gaps for the user organization.

Users have to be mindful of what they're getting from open source, as those tools are built by experts and freely provided to the security community for a specific purpose, but then may never be upgraded or further developed.

In addition, open source tools often don't receive the same scrutiny as those developed for commercial purposes, meaning, they may never be tested by a third party for bugs or vulnerabilities, and aren't subject to audit requirements. Further, when an open source tool is offered free of charge, it may not include all of the necessary features and functionalities. Users are more likely to be forgiving in these cases—these tools have no OpEx cost, after all—but the absence of certain capabilities may result in unnecessary risk. While not every security platform provider has every feature every user could ask for, customers often have sway over development efforts with their commercial security providers.

INTERNALLY DEVELOPED

Another option for SOC and development teams is simply building an in-house cloud security solution. Developers, after all, build software and SOC analysts are security experts. Their combined knowledge could result in an extremely effective solution which includes all organization-specific requirements. But building such tools is time and resource intensive. And, as noted previously, security, in particular, is facing a talent shortage. This may lead to delays or shortcuts that could introduce unnecessary risk.

Plus, just as with open source options, any security tool built by internal teams must be managed and maintained to meet the demands of the current cyber security landscape. Threats and attack techniques happen continuously, so unless the organization can dedicate resources to continuous development of security tooling, buying commercial products is a more attractive options that will save time, money, and effort in the long run.

An additional challenge with build-it-yourself tools is compliance. Many of today's commercial security platforms adhere to major compliance frameworks, even going so far as to map how a tool's capabilities address specific requirements, such as continuous scanning, segmentation, or encryption. What's more, if the DevOps and SOC teams are building security tools that must span both on-premises and cloud environments ("hybrid"), the tools must be adaptable. Security considerations for cloud environments and cloud-native applications are often different from bare metal networks, and thus the builders of such tools will need expertise in both areas to ensure controls are optimally functional in both types of environments and provide uniform coverage across environments.

RECOMMENDED COMMERCIAL OPTIONS

In the cloud security solutions market, there are, broadly speaking, two types of platforms. The first category involves providers that build and expand their own platform from the ground up. The second category is providers that integrate with best-of-breed capabilities. In this section we'll briefly examine the pros and cons of each type.

Cyber security is highly complex. TAG Cyber has developed 54 control categories which fall under six functional areas: Enterprise controls, network controls, endpoint controls, governance controls, data controls, and service controls. End user organizations must pay attention to each of these areas and ensure that they have coverage for each control. While it's impossible to find one tool that affords every security control, orchestration and automation are making it easier for security teams to select platforms that provide comprehensive security benefit.

In the cloud security space, specifically, it's important to look for platforms that were born in the cloud, meaning, they didn't emerge from former on-premises solutions and were recently adapted to cloud as more and more companies responded with additional computer power. A cloud-native focus is

a huge benefit for cloud-first users, as they can feel confident that these providers understand the idiosyncrasies of cloud networking.

ALL-IN-ONE PROVIDERS

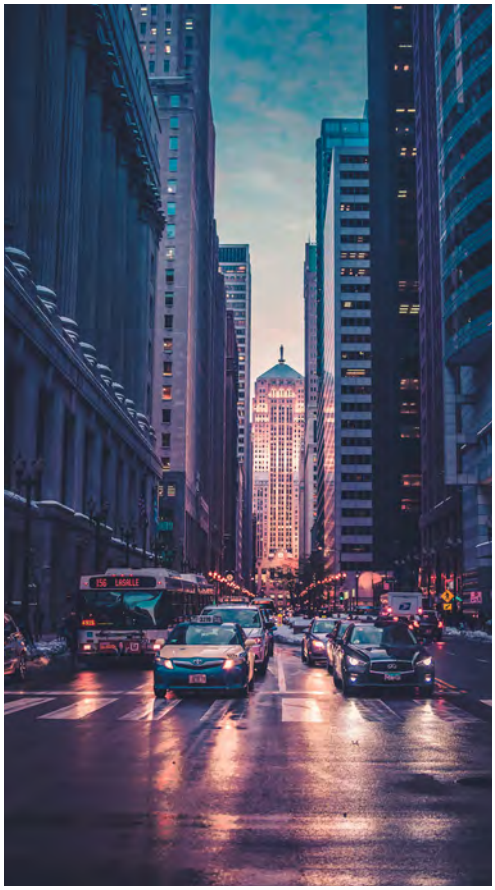
Unfortunately for security and infrastructure teams, there is no all-in-one security provider that can offer capabilities across the entire spectrum, from intrusion prevention to email security, network monitoring to data encryption, and managed detection and response. That said, many cloud security platform providers have combined several capabilities into one platform, making it easy for potential customers to add multiple capabilities with one product installation.

Perhaps the biggest benefit of these all-in-one providers is that the product ships with several out-of-the-box modules that address various aspects of security—identity and access management, intrusion detection, and log management, for instance. This combination of capabilities in one product provides better ease of use than providers which integrate with third-party solutions: Incompatibility issues are unlikely to exist, updating/patching is centralized, there is no need to configure tools separately, and so on.

However, enterprises using all-in-one tools have to be careful of three main things: First, while we're calling these platforms "all-in-one," it's unlikely that any provider can supply a true all-in-one technology, meaning that all required functional areas will be included in one platform, straight out of the box. Therefore, some integration with third-party tools will exist regardless of the efficacy of the platform.

Second, if the security functionality of the platform is broad, for instance, spanning identity, endpoint, and application control, then all-in-one platform providers will need to employ full-time staff for each functional area, which can lead to higher costs passed on to customers. Maintaining expert-level security staff who can build and support each product module and meet customer needs is expensive.

Last but not least, enterprises might be wary of vendor lock-in when using an all-in-one platform. Binding one's organization to a single provider, regardless of capability, could prove problematic if requirements change, if infrastructure changes, if the provider or technology is acquired, or if key management personnel changes.



INTEGRATED SOLUTIONS

On the other end of the spectrum are platform providers that consolidate myriad capabilities via an extensive integration ecosystem. These companies generally focus on building functional capabilities in one area, such as threat detection and response, and then extend beyond the basics by partnering with best-of-breed players in adjacent areas.

The benefit of selecting a platform that integrates solutions is that each component of the platform is purpose built, meaning, they focus on one or two things and they do them well. They're not trying to be an everything to everyone product. This hyper focus often results in superior outcomes for clients.

Very few cyber security companies have the resources to hire and retain top talent in every functional area and thus build numerous solutions from scratch. There are some major players in the space that do, and they should not be discounted. However, most very large companies have grown, at least

partially, through acquisition, in other words, researching and buying best-of-breed players and then integrating the products into their offerings.

With smaller and mid-sized vendors with an integration strategy, vendor lock-in is not an issue, as customers can typically turn on or off individual capabilities or modules and/or swap out a less desirable vendor for another when or if requirements change. APIs make it easy to add or replace capabilities, but the downside is that each component or vendor needs to be configured separately.

Most integration platforms now have bidirectional APIs such that administrators can send data to their preferred platform dashboard, which means that users don't necessarily have to login to yet another tool. However, an API is another potential attack vector for attackers, which should be a consideration in the selection process.

NEXT STEPS AND ACTION PLAN

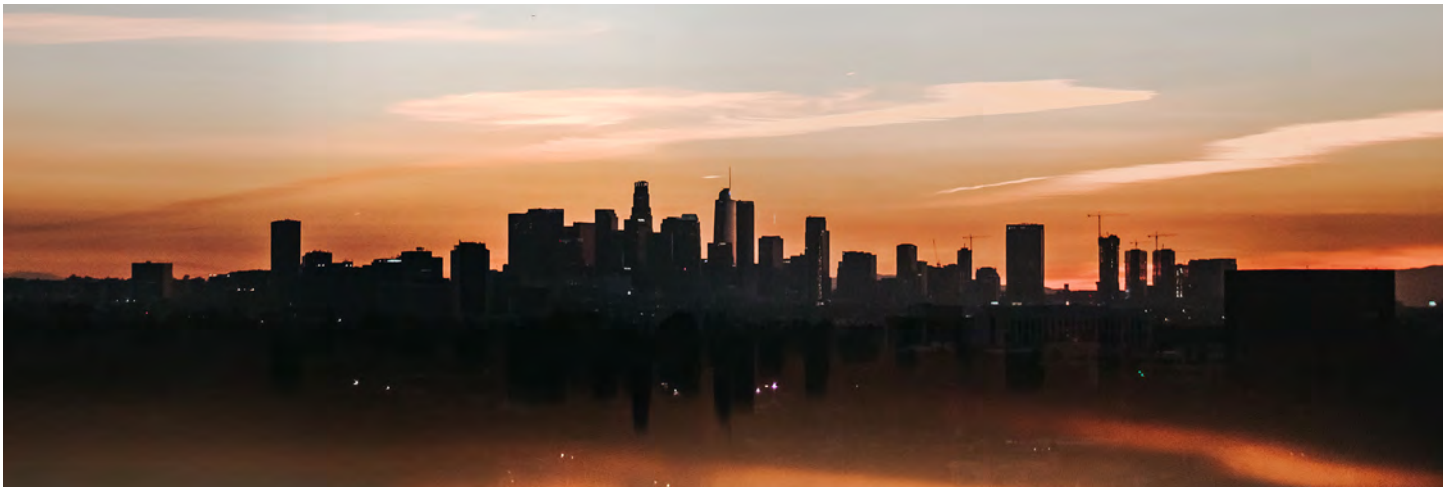
When evaluating cloud security platforms, security and infrastructure teams should look for solutions that work across environments—cloud, multi-cloud, hybrid, and on-premises—and are technology agnostic. Administrators should not need to toggle between views or outputs depending on which environment they're monitoring at the time. The entire concept of a platform is built around ease of use and uniform visibility, and so any potential vendor should be able to provide this capability.

Next, security/infrastructure teams should shortlist platforms that future proof against new technology requirements and developments. Cloud is agile, and emerging technology continuously changes how security teams must protect their organizations. Thus, a selected platform should afford the flexibility to adapt to new circumstances and accommodate evolving data, user, and integration needs.

Another aspect for consideration is how much a chosen platform can demonstrably reduce the amount of noise in the security environment. The increasing number of tools security/SOC teams have deployed can lead to burnout and excessive stress, and therefore simplification and consolidation should be desired traits for any new implementation.

However, noise reduction should not come at the expense of mean time to detect and mean time to remediate. On the contrary, it's imperative for security/SOC teams to quickly identify real threats and act upon them without chasing false positives and low-level events. A tool that offers real-time identification coupled with response capabilities is recommended.

Finally, cloud security platforms should be easy and quick to deploy. Long gone are the days of multi-month deployments; today's security-as-a-service providers are taking the burden out of deployment and delivering value within hours.



FIVE SIGNS THE CYBER SECURITY STARTUP YOU'RE JOINING MIGHT NOT EXIST NEXT YEAR

Every year reams of new companies emerge in the cyber security marketplace. It's a space which fosters innovation, and venture capitalists are eager to back novel companies that might prove to be the next big thing. With the potential for billion-dollar exits, it's no wonder individuals and VCs, alike, are eager to put their stamp on the space with a new tool/product/platform/approach to a problem. And there's plenty of opportunity to do it: Security is a never-ending battle against new (non-security) technologies introduced into businesses, armies (sometimes literally) of cyber criminals with an abundance of time and resources, and seemingly limitless vulnerabilities—from human error to flaws in code to open ports or unmanaged devices on the network. In short, there are many problems to solve and many passionate people who want to solve those problems.

If you're thinking of joining a startup, whether it's your first time or your fifth, here are five "gotchas" to look for to avoid job dissatisfaction, excessive stress, and the need to find another job before you hit your first-year anniversary.

Fueled by digital transformation, cyber security has made its way onto the agendas of quarterly board meetings, mainstream media coverage, and finance balance sheets. This confluence of events has smoothed the transition from practitioner to entrepreneur-with-a-big-idea for many. The market is bursting with possibility, and each year daring individuals take the risk to quit their (probably quite secure) day jobs and build something new. This means that every year there are dozens of new companies and even more nascent companies for job seekers to join. From engineering to engagement specialist, sales to SOC analyst, product manager to platform developer, there's no shortage of hiring in cyber security. (There is, however, a human resource shortage given how rapidly the field is growing.)

For job seekers, especially those with technical skills, the employment options are vast. Everyone must weigh their personal proclivities and preferences to decide if startup life is for them. It's not for everyone. Nonetheless, the opportunity to join a startup, help build something from the ground up, enjoy the perks of a well-funded field, and potentially cash out comfortably in under ten years' time is alluring.

Having listened to hundreds of vendor briefings in the last 9+ months, backed by many years in previous security roles, and bolstered by Ed's insight and experience, I've learned to spot the signals that differentiate the billion-dollar acquisitions and IPOs from the companies that get sold in a fire sale or simply shut their doors after several years in the red. If you're thinking of joining a startup, whether it's your first time or your fifth, here are five "gotchas" to look for to avoid job dissatisfaction, excessive stress, and the need to find another job before you hit your first-year anniversary.

NO UNIQUE VALUE PROP

To level set, "unique" means "one of a kind" or "sole." You can't have something that's "very unique" or "highly unique" or any one of several modified uniques. Therefore, regardless of the company's product or service category—be it network security or IAM or encryption—the company should be able to clearly explain why it is unique, i.e., why no other company can do what it does.

This is tricky, because, realistically, for every company in a category, there are likely several (at least) other companies that do something similar. This can be true on a feature-by-feature basis or it can be true more generally, as in, the security problem they're trying to solve. Either way, if the company cannot define why it is unique, potential customers won't be able to see the value proposition and sales will be scarce. The result? No long-term viability.

On almost every briefing we hear:
- Our product saves time
- Our product solves complexity
- Our product reduces cost
- Our product shrinks the attack surface
- Our product offers full network/endpoint/data/application/etc. visibility

See the problem? There is nothing unique about any of these statements because every startup says them! A company's product or service should approach a problem from a new or different perspective, or why exist at all?

That said, for every security category defined by industry analysts, you can find a small handful to dozens of companies competing. So maybe the product or service isn't unique on a feature/functionality level. That's OK! But if that's the case, the company story should be.

One of the first things Ed's taught me about startup vendor briefings was to ask about the company's story: what it was that made the briefer get up one day, quit their job, and start a new company from scratch. What is their individual story that drives their passion?

This personal story has become even more necessary after hundreds of briefings because, honestly, a lot of companies sound the same via their standard presentation deck. Maybe the company's uniqueness is something in the founders' pasts. Maybe it's their beliefs. Maybe it's their wacky personalities. Whatever it is, find that and you'll understand how the company will compete. Without that, with only a we-save-time-money-effort message, the company isn't going far fast.

A "TOO UNIQUE" VALUE PROP

Call me a hypocrite, but just as concerning as not having a unique value proposition—even if that story is wrapped around some crazy experience that led to the ideation of a company—is a product/service that does something so radically different that no one else is doing it. Is it possible that no one else has thought of the company's particular solution? Absolutely! Is it probable? No. If the company's offering is just ahead of its time, is the product or solution at least addressing an identified problem? Have others in the industry expressed a need to fix X?

For example, in the late 1980s, organizations started noticing a need for a new capability that could monitor and control bidirectional traffic in and out of networks. Networking had evolved beyond the "trusted" and permissive internal network which minimally connected to the outside. This technology, of course, is what we now know as the first-generation firewall. But pinpointing who, exactly, created the first firewall is a challenge. If you were to approach certain security luminaries credited with the invention, most of them will say the seeds were sown somewhere else or that others were developing parallel capabilities. In other words, it was a known problem emerging because of networking trends. And it wasn't relegated to one individual who saw this and said, "I must build a commercial product!"

Said differently, a problem creates the need for a tool, but for a commercial product to be viable, the problem must be bigger than on person's needs. Is it possible that a startup with a crazy idea is soon to be an industry-wide problem? Could be. But too often we see startups fixated on a small issue that won't sell commercially or is really just a feature of an established product. In these cases, anyone working for the company should be concerned about its future.

MICROMANAGEMENT

This section should go without saying, and of course applies to established enterprises as much as it does tiny startups: If the founders—no matter how smart or prescient they are—insist on everything being done their way and don't take outside advice or guidance (or worse, disregard it), run in the other direction.

Startups are all about ingenuity and innovation; a startup that hampers innovation from anyone except a select few executives is bound to fail. Creating something from scratch requires unconventional thinking. Building a product with a unique value proposition demands experimentation and contrarianism. Nothing truly new and novel is ever introduced without some skepticism or objection. Therefore, build teams must be empowered to try and fail at new things—things the founders haven't yet thought of—so they can be market ready.

If you get a sense that the company is built around "my way or the highway," find another company that encourages out-of-the-box thinking.

EPHEMERAL MESSAGING

Have you ever visited a company's website and thought, "that looks interesting," only to come back a few months later to find something entirely different? The company's main message has changed. The product description has changed. What was listed as their product no longer seems to be available or is dramatically different than it was two months ago? While evolution and refinement are mandatory, especially in a startup where the company is finding its footing, concerns arise when messaging seems to change every ten seconds.

OK, "ten seconds" is hyperbolic, but is it not uncommon for Ed and me to talk to vendors every 2-3 months, and there is a not-insignificant percentage of vendors that have a different message every time. They can't seem to nail down what they're selling or how to talk about it. They test wholesale new messaging instead of A/B testing with a select audience. In short, they just don't appear to know who

they are and are pulling at strings to figure that out publicly instead of taking time to define who and what they are.

For these startups, Ed and I ask the company to tell us who and what they are, succinctly and without describing the product or service. If they can't, we offer examples and ask them to try again. If they still can't, we give them an assignment to go off and think about it.

While marketing and messaging should be progressive, it should never be ephemeral—here one day, gone tomorrow. How a company communicates what it is and what it does foreshadows its success and is not something to be taken lightly.

DISMISSIVE OR AGGRESSIVE ATTITUDE TOWARD COMPETITION

Every company has competitors. Even if the company is a unicorn and sells a product no other security professional has yet thought of, but hordes of people are clamoring for, there is competition. The competition might not be a similar product or even a compensating control. The competition could be budget, it could be preconceived notions, it could be inertia. But there is some competing factor for every product or service on the market, especially when it's a new idea.

If you're interviewing with a startup and you ask, "Who's your competition" and company representatives answer, "We don't have any real competition," beware. This company has no idea what it's up against and will struggle. Maybe they'll have a future reckoning, but right now they're not going to be able to handle the inevitable objections by buyers and therefore will succeed only in limited cases, likely through small sales with former customers or friends of the founders.

Similarly, if the company is overly aggressive about its competition, for instance, bashing the competition on the website or in marketing materials, know that the publicly available materials are likely the company's only perceived way to win deals. Every company should be able to demonstrate its value without diminishing others. Comparisons? Yes, buyers need to know points of differentiation, but these comparisons can be done in a respectful way, without making every other company in the space sound stupid.

Can you imagine Roger Federer saying, "I have no true competition" before a Grand Slam? Or when asked about his strengths against an opponent replying with, "His backhand is weak, he is slow on clay courts, and he has no mental resilience after a failed point"? No, because he doesn't need to! He knows he is a great tennis player and is aware of his own strengths and weaknesses. He might say, "He has better footwork than I do" or "My serve is faster and more accurate than his" for a given match, but stating facts is very different than dismissiveness or aggression and, when displayed by a company, should signal a weakness in overall design and demeanor.

THE WRAP UP

Startup life is fun and exhilarating, and the free lunches, company-paid healthcare, and onsite massages won't hurt. But be mindful of company coffeeshop discounts in exchange for an environment that hasn't yet nailed its product space, messaging, or company differentiation. Don't accept unlimited vacation days in lieu of creativity and the ability to personally contribute something meaningful to the security community.

There are many great cyber security startups, and likely one that is hiring (if you're looking). But just like founding a company is a risk, joining one with grim prospects is, too. It can be a real drag to be stuck in a place where you don't see a future, where you're not valued, and where you're always fighting against the tide. Consider these five concerns when evaluating a startup and see if you have a different view of the vendor afterward. You're sure to find several that pass the test with flying colors.

TOP 10 SCAMS TARGETING OUR SENIORS

Every day, seniors in the United States (and elsewhere) are targeted by scamsters intent on stealing their identity, money, and dignity. This note summarizes the top ten means by which seniors are being tricked, and offers suggestions on how this problem might be avoided.

SCAM 1. IRS IMPERSONATION

Criminals generally accuse victims of owing back taxes and penalties. They then threaten retaliation, such as home foreclosure, arrest, and, in some cases, deportation if immediate payment is not made by certified check, credit card, electronic wire transfer, prepaid debit card or gift card. The IRS released the following tips to help taxpayers identify suspicious calls that may be associated with this impersonation scam:

- The IRS will never call a taxpayer to demand immediate payment.
- The IRS will never ask for a credit or debit card number over the phone.
- The IRS will never threaten to send local police or other law enforcement to have a taxpayer arrested.
- The IRS will never require a taxpayer to use a special payment method for taxes, such as a prepaid debit card or gift cards.

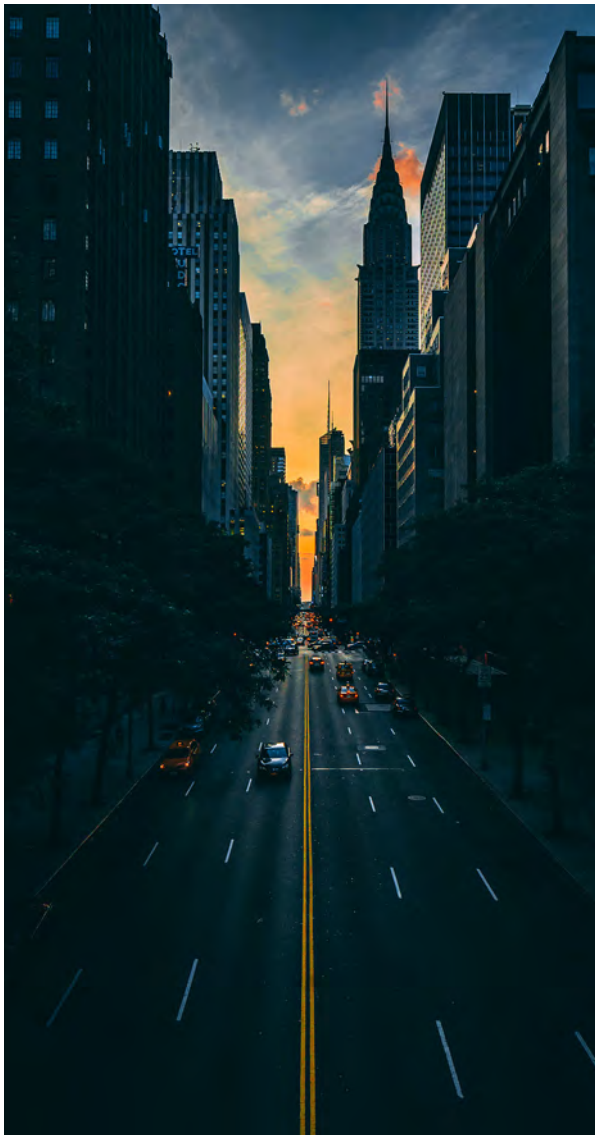
Source: https://www.irs.gov/uac/Five-Easy-Ways-to-Spot-a-Scam-Phone-Call

SCAM 2. ROBO-CALLS AND UNSOLICITED PHONE CALLS

Robo-dialers can spoof the number from which they are calling to mask their identity. Fraudsters make victims believe they are calling from the government or other legitimate entities using numbers that appear as if they are from local area codes. Federal Communications Commission (FCC) has published the following tips for consumers to avoid being deceived by caller-ID spoofing:

- Do not give out personal information such as your account numbers, Social Security numbers, mothers' maiden names, passwords, and other identifying information. Identity thieves often pose as representatives of banks, credit card companies, creditors, or government agencies.

Consumers who search for tech support online may see the number for the scammer at the top of their "sponsored results."



- If you receive an inquiry from a company or government agency seeking personal information, do not provide it. Hang up and call the phone number on your account statement, in the phonebook, or on the agency's website to find out if the entity that called you needs the requested information.

Source: https://www.irs.gov/uac/Five-Easy-Ways-to-Spot-a-Scam-Phone-Call

SCAM 3. SWEEPSTAKES

Criminals contact victims to tell them that they have won or have been entered to win a prize. The victims are told to pay a fee to either collect their supposed winnings or improve their odds of winning the prize. Some helpful tips involve watching for mention of any of the below statements, which must be seen as red flags:

- Hearing that you must act now or the offer will not remain
- Hearing that you've won a free gift but you have to pay charges to receive
- Being asked to provide a credit card or bank account number before you can review the offer

SCAM 4. COMPUTER TECH SUPPORT

Con artists pretending to be associated with a well-known technology company such as Microsoft, Apple, or Dell, falsely claim that the victims' computers have been infected with a virus. Victims are convinced to give remote access to their computers, personal information, and credit card and bank account number so that you can be "billed" for fraudulent services to fix the virus. Individuals searching the internet may see a pop-up window on their computer instructing them to contact a tech-support agent. The pop-up window is used to hack into victims' computers, lock them out, and require victims to pay a ransom to regain control of their computers. Below are several of the most common variations of this scam:

- Victims Unknowingly Contact Scammers. Some consumers unknowingly call a fraudulent tech support number after viewing the phone number online. Consumers who search for tech support online may see the number for the scammer at the top of their "sponsored results."
- Scammers Contact Victims. In the most prevalent variation of this scam, con artists randomly call potential victims and offer to clean their computers and/or sell them a long-term or technical support "service."
- Fraudulent Refund. Scammers contact victims stating that they are owed a refund for prior services.
- Ransomware. Scammers use malware or spyware to infect victims' computers with a virus or encrypt the computers so they cannot be used until a fee is paid.

Some additional helpful tips come from the Federal Trade Commission (FTC) to help consumers avoid becoming a victim of a computer-based scam:

- Do not give control of your computer to a third party that calls you out of the blue.
- Do not rely on caller ID to authenticate a caller.
- If you want to contact tech support, look for a company's contact information on its software package or on your receipt.
- If a caller pressures you to buy a computer security product or says there is a subscription fee associated with the call, hang up.

- If you're concerned about your computer, call your security software company directly.
- Make sure you have updated all your computer's anti-virus software, firewalls, and popup blockers.

SCAM 5. ELDER FINANCIAL ABUSE

Financial exploitation of older Americans is the illegal or improper use of an older adult's fund's property, or assets. Most victims are between the ages of 80 and 89, live alone, and require support with daily activities. Perpetrators include family members, paid homecare workers, those with fiduciary responsibilities (such as financial advisors or legal guardians), or strangers who defraud older adults through mail, telephone, or internet scams. The GAO identified several measures that can be taken to protect seniors from guardianship abuse.

- Including for courts to ensure that a guardianship is truly needed before appointing one and periodically reexamining whether a guardianship is still needed.
- Courts should also make sure that guardians are screened for criminal backgrounds and are properly educated on their role and responsibilities.

SCAM 6. TARGETING GRANDPARENTS

In this scam, imposters either pretend to be the victims' grandchild and/or claim to be holding the victims' grandchild. The fraudsters claim that grandchild is in trouble and needs money to help with an emergency such as getting out of jail, paying a hospital bill, or leaving a foreign country. Some helpful tips include the following:

- Independently identify the story.
- Hang up and immediately call the relative who is asking for your help. Do not use the number they provide, use your own contact information that is on file.
- Verify the whereabouts and story with another relative of the person who needs your help (parent, sibling etc.).
- Do not keep the situation a secret between you and the person needing assistance.
- Do not send money that uses a special payment method, prepaid debit card or gift cards.

SCAM 7. ROMANCE

Typically, scammers contact victims online either through a chatroom, dating site, social media site, or email. The con artists will ask their victims for money for a variety of things such as travel expenses, medical emergencies, hotel expenses, hospital bills, or losses from a temporary financial setback. Some helpful tips from the FBI's Internet Crime Complaint Center to help prevent consumers from falling victim to romance scams include the following:

- Be cautious of individuals who claim the romance was destiny or fate, or that you are meant to be together.
- Be cautious if an individual tells you he or she is in love with you and cannot live without you but needs you to send money to fund a visit.
- Fraudsters typically claim to be originally from the United States (or your local region) but are currently overseas or going overseas for business or family matters.

Source: https://www.fbi.gov/news/news_blog/2014-ic3-annual-report

SCAM 8. SOCIAL SECURITY IMPERSONATION

This involves consumers receiving calls or emails from individuals claiming to represent the Social Security Administration (SSA). The caller generally asks for personal information such as Social Security number, date of birth, mother's maiden name, and/or bank or financial account information. Some helpful tips to help secure your identity:

- Social Security will not call to ask for your bank account information or SSN.
- There will never be a fee charged to obtain a Social Security card.
- Social Security numbers do not get suspended.
- Never give out personal information over the phone to someone you do not know.
- Don't be afraid to call SSA's Inspector General at their toll-free number (1-800-772-1213) to verify the caller/request.

SCAM 9. IMPENDING LAWSUIT

Like the IRS impersonation or Social Security impersonation scams, the impending lawsuit scam typically involves consumers receiving calls from individuals claiming to be from local, state, or federal law enforcement agencies. Consumers are told that there is a warrant out for their arrest, and unless the person agrees to pay a fine, they will be immediately arrested. Some helpful tips include the following:

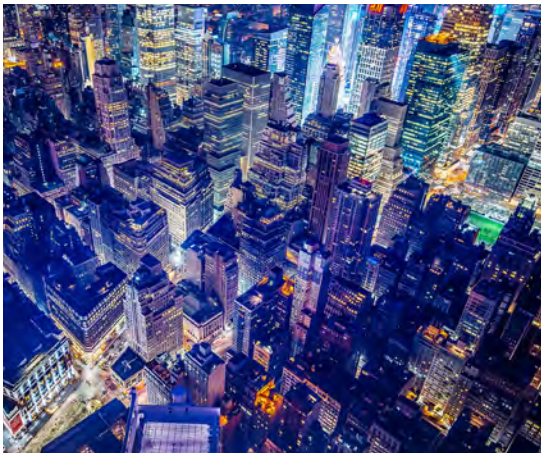
- Law enforcement will never call to demand immediate payment.
- Law enforcement will never ask for a credit or debit card number over the phone.
- Law enforcement will never require you to use a special payment method for taxes, such as a prepaid debit card or gift cards.

SCAM 10. IDENTITY THEFT

Identity thieves disrupt the lives of individuals by draining bank accounts, making unauthorized credit card charges, damaging credit reports; they often defraud the government and taxpayers by using stolen personal information to submit fraudulent billings to Medicare or Medicaid, or Social Security benefits.

Some helpful tips and what to do if you suspect you are a victim of identity theft:

- Visit the Federal Trade Commission (FTC) website on identity theft (https://www.identitytheft.gov/)
- Call the companies where you know the fraud occurred



- Place a fraud alert with a credit reporting agency and get your credit report from one of the three national credit bureaus
- Report identity theft to the Federal Trade Commission
- File a report with your local police department
- Closed new accounts opened in your name
- Remove bogus charges from your accounts
- Correct your credit report
- Consider adding an extended fraud freeze

Source: https://www.identitytheft.gov/

SHOULD A LAW FIRM PROMISE THAT A CLIENT'S DATA WON'T BE HACKED?

In the beginning, cyber security was all about prevention. Then everyone agreed that it wasn't possible to prevent cyber attacks. The experts acknowledged that it happens to the best of them.

"It's not *if* but *when*" was the new reality. There was also another way of putting it. "There are two kinds of companies: those that have been hacked, and those that don't know it yet."

The demonstration of strength was how a company reacted *after* the inevitable breach—which showed how resilient it was. That's where we seem to be now. But does this rule of thumb apply to everyone—including law firms?

Lawyers are not known for being tech savvy. They would be wise to exercise care when they make promises in this area.

Should it? Should a law firm let clients know that it's impossible for *any* company to promise that there won't be intrusions?

One law firm went the other way. Not only did it skip a disclaimer, it told a client it would protect his data from cyber attackers. And now it finds itself facing a lawsuit that cleared a motion to dismiss.

The suit was unusual in several important respects. It was a high-profile case with international repercussions. The client had anticipated that his information would be targeted by attackers. He specifically asked that his data be stored where it would not be vulnerable to attack. And he apparently received assurances that it would be.

The client was Guo Wengui, and he had good reason to fear he would be the target of cyber criminals. A Chinese real estate developer, investor, and billionaire, Guo had fled China as a self-described whistleblower and dissident in 2015. Now 50, he has been living in the United States and Europe ever since.

In an opinion filed in late February, District Court Judge James Boasberg of the District of Columbia found that Guo had been threatened by the Chinese government after he exposed systemic corruption in his homeland. And the Chinese government orchestrated further harassment against him in the United States, the judge wrote. That led Guo to seek political asylum.

In 2016 he hired Thomas Ragland, a partner at Clark Hill, PLC, to represent him in his application for asylum. And he warned his attorney that, as a prominent Chinese dissident, he had been subjected to persistent cyber attacks, and that more should be expected. Ragland and his firm agreed to take "special precautions" to prevent disclosure of his sensitive information, Boasberg wrote, and the information would not be placed on the firm's computer server, "as doing so would make the information more vulnerable to hackings."

The following year, the law firm's network was indeed hacked. Both sides agree that China was responsible, and the attackers obtained "a substantial amount" of personal information about Guo and his wife. They also obtained his asylum petition, and they published all of it on social media.

Clark Hill and its lawyers withdrew from the case. They explained to Guo that they had to, since they might be called as witnesses in his asylum proceeding and that would create a conflict if they continued to serve as his advocate.

Guo sued, alleging that the firm and Ragland had breached their fiduciary duty, breached their contract with him, and had committed legal malpractice. He also asked for punitive damages. The defendants moved to dismiss all counts, arguing that Guo had failed to state a claim. Neither the withdrawal nor the attack was a ground for legal malpractice, breach of fiduciary duty, or breach of contract, they argued. And even if the allegations were true, the cyber attack did no harm.

THE JUDGE'S REASONING

Boasberg found that Guo had sufficiently pleaded that the defendants breached their duties of loyalty and good faith "by misrepresenting the manner in which they would protect his confidential information in order to secure his business." They put the information on their server "and conveyed it via a firm email account—*in direct* contravention of his instructions," the judge wrote. And Guo's complaint also included details about the damage he had suffered, leading Boasberg to reject "defendants' invitation to find that the cyber attack did not actually harm plaintiff as a matter of law."

The judge added: "Discovery may reveal that defendants never made any such misrepresentations to plaintiff and were not negligent in their handling of his confidential information, but the well-pleaded allegations in the complaint preclude granting defendants' motion to dismiss."

Boasberg also allowed the malpractice claim to stand. The law firm failed "to use the required degree of professional care and skill in representing plaintiff" and failed to maintain "reasonable security measures to secure their computer system from unauthorized access, as required and promised to plaintiff." For similar reasons, he refused to dismiss the breach of contract claim.

The judge dismissed the remaining claims. The law firm explained it was obliged to withdraw from the representation, citing rules of professional conduct. Boasberg didn't need to consider that argument, he said, because Guo failed to show how the withdrawal harmed him. And the judge quickly dismissed punitive damages, which "are a form of relief, not a stand-alone cause of action," he wrote. Moreover, they require the violation of plaintiff's rights in an "intentional, deliberate, [and] outrageous" manner,

which Guo did not actually allege, the judge concluded.

The case, previously reported by Bloomberg, still has a ways to go before it's resolved. But it's not too soon to draw lessons.

Don't make promises that you can't keep. If you guarantee that documents will be secure, that's tantamount to promising that they won't be shared on the internet—as Clark Hill apparently did. But it's hard to function off the grid. It's *possible* to mail and fax documents, but that's not expected or necessarily appreciated by lawyers and judges. In fact, some courts require electronic filing.

Even in courts that don't, this may not be possible to control. If one lawyer makes a promise, he may find it difficult to be sure that everyone involved will follow suit, including partners, associates, paralegals, secretaries—and lawyers on the other side.

As a group, lawyers have not been known as leaders in the world of technology. In fact, they've been known as laggards. The best policy for most is probably to under-promise and aim to over-deliver. Otherwise, they may end up practicing their litigation skills on the wrong end of a lawsuit.

A 'COME TO JESUS MOMENT' FOR LAW FIRMS

For a while there, law firms seemed to think it was OK to advise clients about cyber attacks without considering their own vulnerabilities. Sure there had been some very big breaches, like the so-called Panama Papers case in 2016 that led to the demise of the Panamanian firm Mossack Fonseca & Co. But that was so far away.

The DLA Piper take-down a year later was a little closer to home, but that turned out to be part of the vast NotPetya cyber attack. There were other, smaller attacks that involved law firms based in the United States that received less publicity.

Law firms that have hired chief information security officers and have given them real power are often firms that have been breached themselves.

The ransomware attack in May that struck New York's Grubman Shire Meiselas & Sacks was different. It was high profile well before it was revealed that the attackers were demanding $42 million. That was because they threatened to sell documents that belonged to the firm's glittering roster, which included Lady Gaga, Madonna, Bruce Springsteen, and supposedly even President Trump.

That should have given law firm partners everywhere a jolt. It underscored the opportunity that one law firm can present to enterprising cyber criminals. It's not the law firm's own documents that are so appealing—it's the opportunity to steal intellectual property from hundreds of the firm's clients. And firms may be particularly tempting targets because many have less than stellar security. Once attackers get in, they may find clear sailing with few protections in place.

On top of that, many firms are particularly vulnerable to business email compromise. Why? Because of their culture. Business email compromise involves emails that seem to be coming from top executives but are actually coming from threat actors. When law firm staffers receive emails ostensibly sent by top partners, the hierarchical culture of absolute authority dictates that they respond quickly and without question. Including when the instructions are to wire funds.

This poses a real security problem. It's exactly what cyber criminals want. Firms need to change their culture through training. No one should assume that instructions came from the person who purportedly sent them. Before they follow orders that include actions like wiring money, lower level employees need to demand proof of the individual's identity and the veracity of the request. And their bosses must empower them to do this.

John Strand of Black Hills Information Security said he has recently seen changes in law firm attitudes toward security. But it's not just from reading stories about law firms that have been hacked. The ones that seem most interested in hiring chief information security officers and giving them real power are firms that have suffered breaches themselves. That "come to Jesus moment" seems to carry a lot of weight.

Strand has found that the penetration testing that his company and others offer can simulate that moment—without inflicting the damage. This can be especially effective in the current climate, when the dangers of breaches are publicized daily. Pen testing may not be representative of a real-life threat (that's what red teaming is for), but it will uncover vulnerabilities in firms' systems, including those that are driven by human actions like clicking on a suspicious email, and highlight to partners why it's important to take cyber protection seriously.

6 TIPS FOR SECURING FUNDING FOR YOUR SECURITY STARTUP

The cyber security products market seems to be a never-ending stream of companies emerging on the scene to solve an unsolved problem, remedy an issue from a unique angle, or define an untapped market segment. Every year we see clusters of companies launch in a new category. In recent years it's been endpoint detection and response (EDR), cloud access security brokers (CASB), zero trust, deception technology, security orchestration, automation and response (SOAR), and the list goes on the farther back in time you go. Some of these products and companies hit it big, growing over the years into a household name, and some get gobbled up through acquisition by a well-known enterprise. And while the technologies and problems they address vary from one company to another, they all have one thing in common: they begin as a startup.

There is no one formula for founding, building, and running a cyber security company, but many startups seek venture capital (VC) investment to get off the ground floor. From financial investment to advice on messaging and positioning, a VC firm can be a treasure trove of information for eager founders. .406 Ventures is an early stage technology investment firm that has helped many recognized security brands rise from their humble beginnings. With deep expertise as business owners, operators, board members, managers, and (of course) investors, the team has a honed perspective on what makes startups successful.

Recently I spoke with Greg Dracon, .406 Partner and cyber security practice lead, and Rob McCall, Associate and cyber security practice member, about the security startup market and how companies seeking investment—and a growth strategy partner—can best position themselves.

MARKET EVALUATION

There are thousands of cyber security vendors, and not only startups look for investment, strategic advice, or go-to-market support. How does .406 sort the wheat from the chaff? Most investments (upwards of 70% in .406's case) start with the team's personal and professional

Every year we see clusters of companies launch in a new category.

networks, explained McCall. Tapping into friends, colleagues, industry advisors and board members, prominent CISOs, and end users allows them to find companies solving identified market problems at the ground level. That's not to say an unknown commodity cannot earn the attention of a VC, but having a warm lead or soft intro from a trusted source helps companies break through the noise and may give the VC an extra bit of confidence in a founder. In short, never underestimate the necessity of a strong network.

With so many companies developing cyber security products, it can be hard to surface the crystals that will become diamonds over time given the right market conditions, even if they come with a strong recommendation. "This is the hardest part of our job," said Dracon. "Security used to be based 100% on the technology—is it more effective than existing solutions? How does it work?—but today, cyber security is more mainstream and needs to solve business problems alongside technology problems. When evaluating companies for investment, we need to see that the founders not only understand security, but that they have a good understanding of how to build a successful business and that they're just as focused on sales and marketing as they are building a product or platform."

The platform is also a key component; Dracon said that while point products can fill a gap and grow into an extensible solution, as investors and partners, .406 wants to work with founders that see the bigger picture: how a company and its platform can be extended over time, build additional value for customers, and is sustainable as market needs change (which they will).

OUTSTANDING CHARACTERISTICS

A promising product idea and mutual network connection may secure an initial meeting, but no VC is going to award millions of dollars to an entrepreneur simply because someone spoke well of them. "To consider an investment," said McCall, "we need to see a combination of good technology and a founder with vision. Is this person a former operator that lived the problem day-to-day and now wants to build a solution? Do they understand the market holistically, from real and perceived competitors to market opportunity? Are they capable, adaptable, and receptive to change based on external factors? Are they willing to take advice and constructive feedback? Can they inspire and lead a team?"

Dracon built on this last point and added that the willingness to work with a team is key: "Successful entrepreneurs come from all different backgrounds. Management teams that work well together, have similar principles, have mutual respect and trust, and have good leadership capabilities are more likely to see success. Acknowledging one's own weaknesses and seeking to hire those with complementary skill sets is very important to us as a CEO characteristic."

Other important, albeit less tangible, characteristics .406 looks for in a startup is a founding team with passion, integrity, and a commitment to sticking it out through tough or unpredictable times. The road to success will rarely be easy, and founders who approach building a company realistically but with wholehearted dedication are more likely to turn their idea into something big and sustainable.

But there is a catch: Both Dracon and McCall said that .406 is not looking for "quick flips." Though cyber security is a highly opportunistic market and founders hope to make millions off an acquisition, acquisition shouldn't be the primary reason or overly analyzed when building a company, at least not for founders who want to work with .406. Dracon and McCall told me that the firm has a saying that goes something like: "Build the company as if you'll own it forever or you will." If you build something valuable and sustainable, opportunities to monetize will inevitably surface. True enough, there are easier and faster ways to make money than developing a cyber security tool to sell in an overcrowded market.

THROWING YOUR PITCH

When I asked Dracon and McCall for their "top tips for pitching a VC," they originally alluded to three pieces of advice. Those three bullets turned into six, and given their experience and fact that they listen to nearly two thousand (!!) pitches every year, they could probably come up with more. But here are the top 6 things to keep in mind if you're thinking of approaching a VC:

1. Use your network to try to find a connection to the VC firm and ask for an introduction. With thousands of companies knocking on their door, an endorsement from a mutually trusted source will help you bubble to the top.

2. Be targeted about which firms you're approaching and do your research. Different VCs have varying interests and areas of expertise. Make sure your company fits into the VC's strategy and get to know a little about each person you are pitching. Align backgrounds and experience and make it personal—because a startup is more than business.

3. Know your market thoroughly, including the competitive landscape, market sizing, trends, target buyers, and potential partners. Demonstrating this knowledge will show the VC that you've invested in the business side of your company, not just the product or technology.

4. Get your back office in order. From your financials to your sales deck to answers about operating procedures and team members, a VC wants to know the company they're investing in is organized and is capable of managing a successful business, not just building a better widget.

5. Be open, honest, and respectful. Your eventual VC is going to be a partner in addition to financial supporter. They want to learn your expertise and vision, but also need to see and hear that you're willing to accept critical feedback, that you are truthful in representing the company, and can course correct when necessary. Acting like a know-it-all, dismissing the knowledge of others, or misrepresenting the company or market opportunity will be apparent and won't serve you well.

6. Treat meetings as a two-way evaluation. The VC may be the one supplying the influx of cash, but that means they're going to be by your side for many years to come. Do members of the team have the right expertise and sector focus to help your business? Do they know your market inside and out? What does the rest of their portfolio look like? Will they have enough time to dedicate to your company?

THE WRAP UP

Most cyber security startups and many established players seek outside investment. Approaching and pitching a VC firm should be treated as seriously as which features and functionalities you will include in your product(s). You'll need a solid foundation and a lot of business savvy to earn investment from a top-tier VC, so do your homework! And look for a firm that will be more than just a financial backer that can get you name recognition.

If you're thinking about pursuing an investment, you can learn more about the process in this video featuring Maria Cirino, .406 Ventures' Co-founder and Managing Partner, or connect directly with the team.

IS THAT AN UNPROTECTED PHONE IN YOUR POCKET?

Close your eyes and picture this: You've finally managed to take that long-awaited, well-deserved vacation-of-a-lifetime with your partner/spouse/BFF. You're overlooking the Mediterranean Sea/watching majestic elephants roam through Kruger National Park/enjoying the vista from atop Matterhorn. Envision how peaceful it is, how excited you are to finally experience the sights and sounds around you. You are immersed in the moment.

And your cell phone chimes. Oh, look. It's a call from a telemarketer.

The daily struggle to be connected and secure, to exercise the right to carry your devices but disconnect is real.

Try this next scenario: Your employer has sent you on a business trip to China/Russia/Saudi Arabia/Malaysia and you need to protect your devices and communications from surveillance. It's impractical to buy and configure temporary devices to have only minimal information stored on them, and any communication back to "home base" can still be tracked and/or recorded…if you're a target.

Last but not least: You're a security expert and you love technology! You have several phones and multiple computers. They're all secured to the hilt—you have long, complex, unique passwords for every site/app/account. You carry around your YubiKey. You have premium subscriptions to top-rated malware scanners. Everything is encrypted. You'd never use a home assistant. Location, NFC, and Bluetooth are disabled whenever possible. But since you're a security expert, you understand that no connected technology can be easy to use and 100% secure, and it doesn't take a security genius to know that tracking is occurring at every turn we take.

Maybe you're paranoid. Perhaps you feel, as many of us in the security community do, that it's our responsibility to protect our devices and privacy as much as possible. Perchance you realize that disconnecting for periods of time is healthy for your body and mind. Whatever the scenario, there are numerous, legitimate instances where people need to carry connected devices or simply feel better carrying devices (I'm being chased by a rhino! Send help immediately!), but also want or need to make the devices inaccessible and just turning them off won't do the trick (The rhino isn't likely to digitally surveil you, but a government might).

DEVICE CONVENIENCE WITHOUT SIGNAL INTERCEPTION

The daily struggle to be connected and secure, to exercise the right to carry your devices but disconnect is real—which is why in the last ten or so years we've seen a surge in the number of companies producing Faraday cages that block wireless signals, shield devices and documents from RFID/NFC, and protect you from radiation and other electromagnetic frequencies. A quick Google search will tell you that Faraday products aren't exactly in short supply, but who wants to look like a Doomsday Prepper when carrying a laptop bag or while hiking the Himalayas? Even the geekiest of security geeks sometimes want to be geek chic.

A crop of fashion-conscious companies like Silent Pocket, Tech Wellness, and Lambs offer products that are well made and high quality but also afford a subtle, discrete technology with an embedded feature that allows people to disconnect.

Security and privacy wonks understand the need to keep private information, well, private and secure, so I won't spend much time in this post extolling the virtues of a Faraday cage. Suffice it to say, we all need our devices to function, but when and if we don't need them to be on or when we're concerned about unauthorized access, isn't it sensible to make them inaccessible to potential lurkers?

Let's say you're walking the Black Hat/DEF CON/BSides LV conference halls at some point in the future; you're going to have your devices with you. You're going to need to use them, and presumably you're not connected to the conference wireless, Bluetooth, GPS, NFC, etc. and your VPN is always on. Still, your connection can be intercepted. If you don't believe me, just sit through one of the end-of-event NOC reviews. Instead of throwing your device into your conference backpack and exposing yourself to becoming the highlight reel of "traffic we observed during XConference," you could throw your device into your new blue light blocking backpack and feel confident the guy with the WiFi pineapple isn't snooping.

HEALTHY VIBES

The other, and of no lesser importance, benefit to using Faraday products for your devices is something many of us don't think about enough: health and wellness. To function, devices need to emit signals, and those signals expose us to low doses of electromagnetic radiation that could adversely affect our health. Perhaps that's a little too hippy for you. Research shows that device usage has negative effects on our sleep, can cause muscle pain, strains our eyes, and stresses our brains. In fact, new research suggests that overactive neural activity, which can be induced by stress, overthinking, and lack of downtime can shorten humans' life spans.

It's not new news that disconnecting is good for us. It's not a groundbreaking idea that being in nature or painting a picture or dancing or singing—activities which don't require electronic devices—reduce our stress levels, allow us to relax, and make us more productive, creative human beings! Yes, tuning out for a while each day makes us better people and better employees. Still, the temptation to reach for our phone, to send a text, to check our work email to prove to our boss how valuable we are, nags at us every minute, especially when we can hear that notification sound.

Will putting your devices in a Faraday bag/wallet/briefcase/tablet sleeve force you to not use your tech and be one with nature or talk to your family more? No, in many cases you'll still have your devices on your person. However, removing the constant reminder of emails, texts, and app notifications by disabling connectivity entirely takes away the pressure to respond or follow up on "just this one message…"

BEYOND THE FEAR OF PHISHING: SECURITY TRAINING FOR THE HUMAN LAYER

The first time I became aware of phishing was in spring 2000. The startup I was working for had just hired new employees and the eight of us were working out of temporary office space. One of the new hires, Mike, was settling in, setting up his email, learning our CRM tool, and starting to prospect his territory. Although our local office was tiny (in size and number of people), we were part of a larger organization with offices and employees across the US. It was therefore not unusual—or suspicious—to receive an email from an unfamiliar colleague. When Mike received an email "from" a colleague, although the subject line seemed odd—it read "ILOVEYOU"—Mike clicked, not wanting to ignore his new coworker. The email content instructed Mike to open an attachment, and … you know what happened next: The "Love Bug" spread to every contact in Mike's address book, including the CEO.

. . . you know what happened next: The "Love Bug" spread to every contact in Mike's address book, including the CEO.

Because it was 2000 and because little information was on or accessible by Mike's machine (he'd just started and we had only local access to the CRM database) minimal damage was done. Mike was embarrassed, but the IT team was able to contain further internal spread and prevent important files from being corrupted or deleted. Not every company was so lucky, and the "Love Bug" introduced the dangers of phishing to the average worker's consciousness.

For several years after "LoveBug," phishing remained a prevalent scam, but one that was recognizable. Silly subject lines, like "ILOVEYOU" were the norm, obvious grammatical mistakes were rampant, and requests within the email body were often huge tipoffs (No, you don't have a long lost uncle from whom you will inherit $10 million if you just click on this link and pay $100 first). Yet, these phishing scams worked—and still do.

At the same time, awareness about phishing was on the rise. Companies warned employees about the insecurity of clicking on links and opening attachments, and IT and security teams deployed email security tools and anti-virus to help reduce what could get into or out of the organization. As companies got better at filtering out the obvious, scammers got better at creating campaigns that could evade detection. Employees no longer had to be on the lookout for a Nigerian prince; now, HR professionals had to be wary of resumes attached to emails, finance professionals needed to be suspicious of requests for payment information, and logistics teams couldn't blindly open emails with information about a missing or delayed shipment. The game was increasingly more sophisticated.

BEYOND SECURITY AWARENESS

By the end of the decade, phishing had become the top vector for exploit by cyber criminals, yet companies couldn't rely on busy employees to identify every threat, and current technology wasn't doing enough to prevent malicious emails from landing in employees' inboxes. In 2020, all that has changed. There are multiple, capable and effective technologies on the market to help stop phishing threats and mitigate endpoint vulnerabilities, and numerous security awareness training platforms to help organizations in their endeavors to reduce human layer risk.

Today, security awareness training is considered a staple of cyber security programs. All the technology in the world won't eliminate breaches if a determined attacker can exploit a human being at the end of a device. It's therefore been a long-held belief in the security practitioner community that enterprises need to provide security training to employees, often once or twice per year mandatory classroom sessions complemented by more-frequent online assessments. At times, these programs have been positioned as combatting the problem that "humans are the weakest link," which doesn't do much to help employees feel like they're an important part of the process. In better cases, where awareness training is presented from a more positive perspective, enterprises trumpet increases in reporting, decreases in risky behavior (such as clicking on links in emails from unknown senders), and even a reduction in malware slipping past the endpoint.

While the latter is a desired outcome, there is often a limit to how much these programs affect. For one thing, when awareness training is infrequent or when it's offered as a pre-packaged solution, employees may feel like they have to complete the activity to check the box that says they did X so they can get back to their "real" responsibilities. Conversely, when the organization treats security awareness training like a compliance activity, little effort may be put into emphasizing its importance or benefits, especially on a personal level. Last but not least, when the focus is on correct answers rather than behavior, potential improvements may be buried under apathy.

I've written before that awareness isn't the problem in security. Three years later I still believe this to be the case. Maybe even more so. Today, your average device and internet user knows about cyber security risk. Heck, most of them have been part of some breach of their personal information. If you're testing awareness, your employees are probably going to fare fairly well. In the heat of the moment, though, that's when things get tricky. And that's why the focus must be on behavior change and must be tailored for the individual rather than the company the individual works for.

SAVE YOUR PROCLAMATIONS OF LOVE

Today, phishing has progressed far past Love Bug-type campaigns, which is why it's so hard to stop its success. Many endpoint or email gateway technologies can identify low-hanging fruit—more-obvious phishing campaigns and those already observed in the wild. But it takes more than simple technology to combat today's phishing threats. Although we all endeavor to love working for our bosses, no one wants to profess their love through a clumsily-crafted email containing the gift of malware.

Attackers are known to use sophisticated techniques and convincing tactics—some even employ marketing and design personnel—thus defenders need to fight back using equally sophisticated technology and user training.

The key, then, is finding a technology partner with products or platforms that focus on behavior change, and where individual employees' training modules can be tailored to their needs—not the needs of like employees or departments. The data collected by the product/platform should be specific enough to allow administrators/trainers to present the appropriate lessons for the individual and doesn't make them feel like they're taking a test to pass the test.

If security awareness training is meant to help humans be the best and first layer of defense against your organization's cyber threats, then the solution(s) you chose should be human-layer solutions: those which understand the behavioral aspect of how phishing and social engineering succeed, and those which focus on behavior at a personal level. No human likes to feel like they're being churned through a meat grinder, which can happen when training is too generic or treated as a compliance requirement. No one likes to feel like stupid, which happens when there is a message that "users are the weakest link."

VENDOR ANALYSIS

When evaluating human layer security vendors, don't be afraid to ask them about their approach: Do they still have the mindset that employees are the weakest link that needs to be patched, or do they believe in progressive training that focuses on behavior change? Can their product/platform be customized to each user's needs based on the data collected or is it one size fits all? How much automation is built in? What about threat intelligence on current human-focused attacks?

Reducing cyber risk to enterprise resources requires a combined focus on malicious threats to process, technology, and people. The cyber security industry is dominated by commercial solution offerings that address process and technology risk. Instead, when it comes to human layer security and combatting phishing and other endpoint vulnerabilities, look for people-oriented solutions that are designed to help employees make better security decisions.

THE IMPORTANCE OF CONNECTING TO BUILD CYBER SECURITY

An eclectic Manhattan conference touches on CISOs, sales, comic strips and robots. There was even a retired four-star general.

What is most vulnerable about the nation's cyber security? "We have essentially a reactive capability. We wait for something to happen, and then we react." That was the assessment of retired four-star general Keith Alexander, who was director of the National Security Agency from 2005 to 2014, and in 2010 was appointed first commander of the United States Cyber Command, charged with defending the country's security in cyberspace.

The real problem, Alexander said at a cyber security conference in December 2019, is that everyone is operating independently. Everyone is defending their own. There isn't enough coordination. "Imagine crowdsourcing our threats," he said. "Our level of protection would be magnitudes better than it is today."

As gloomy as some of his words sounded, Alexander found reason for optimism. There's a lot of talent in finance, in telecom, in a number of industries that can aid the government's efforts, he noted. "This area is going to change dramatically in the next 24 months," he predicted. "There are a lot of things we've got to fix in our country, but cyber is one we're *going* to fix."

Alexander is now co-CEO of IronNet Cybersecurity, which he founded in 2014, shortly after he retired from the NSA. The firm's mission is to help bring companies and industry together in a collective defense to leverage advanced network traffic analysis and enable the sharing of threat intelligence.

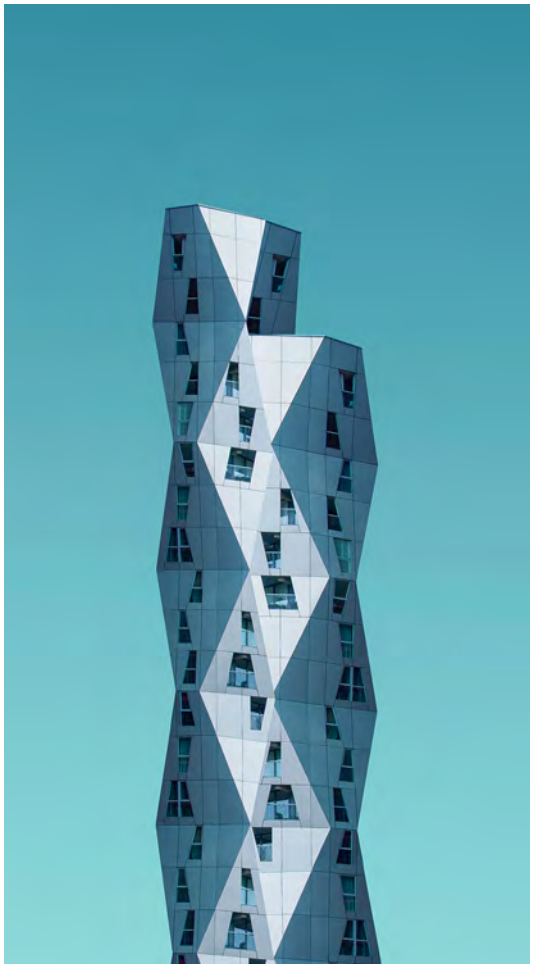
He was speaking at a conference in Manhattan put on by TAG Cyber, a consultancy founded in 2016 to offer coaching, research and guidance to tech teams focused on cyber security. Sitting next to Alexander on the stage was Ed Amoroso, the firm's founder and CEO. Amoroso, who holds a doctorate in computer science, teaches at New York University and Stevens Institute of Technology, and worked at AT&T for 30 years, the last 17 as chief security officer.

The two men have been friends for years, and there was an easy camaraderie in their conversation. Amoroso had started by asking Alexander how he found his way into the Army. "I'm pretty sure that everyone here had the options that I had: prison or the military." After the laughter subsided, he continued: "You get uniforms. Meals." (Spoiler alert: He actually went to West Point.)

Alexander's presentation continued to be leavened with humor as he recounted career highlights, but later he dropped the self-deprecation. His most dramatic story involved Operation Overt in 2006—a security operation to thwart a terrorist plot originating in the U.K. to blow up planes using liquid bombs.

He had just finished reading all the "traffic" that had come in. And then he joined a meeting. Bush, Cheney, Rice and the others were on a screen, looking "like Hollywood Squares," he said. He didn't realize that he would be their "briefer" that day—until the president suddenly said to him, "Tell us what's going on."

Does he miss those days? Does he miss the NSA? "I do miss the people," Alexander said. Asked about his transition to the private sector, he said that it's important to have big goals: People get excited when you tell them, "We're going to solve this problem." And you need to show them that you're "all in." It's also important to invest in people, as he'd done in the military. The attitude should be: "We're hiring these people not to tell them what to do," he said. "We're hiring them to ask them what *we* should do."



A MIX OF SPEAKERS

Earlier in the day, Amoroso had opened his fourth annual conference by welcoming the 120 invited attendees, most of them cybersecurity vendors, and reminding them that his events were not like the ones they were used to. His were all about ideas, he told the crowd, not commerce. No big screen. No booths. No PowerPoints. Just talk. But not all of it from grizzled veterans. Amoroso had gathered an eclectic mix.

First up was Robert Hackett. A senior writer at Fortune magazine, where he has worked for five years, Hackett writes a column on cyber security and covers emerging technologies. He estimated that a third of his work is devoted to fintech, a third to science and a third to cyber security. He and Amoroso were joined onstage by Katie Teitler, a TAG Cyber senior analyst.

Teitler asked Hackett about privacy, wondering whether we're now forced to trust companies with all of our data. "It's a scary world out there," Hackett acknowledged. He recommended a book about the data economy called "The Age of Surveillance Capitalism," by Shoshana Zuboff.

What about a federal privacy law? Teitler asked. Did he expect one that would push beyond the California Consumer Privacy Act? A federal law will likely pass that supersedes the California law, though it will also likely be weaker, Hackett predicted. Regulation will favor incumbents, making it harder for startups to compete. In the last century, telecom regulations allowed AT&T to enjoy a government-sanctioned monopoly, and today's big tech companies would be happy to have something similar, he added. "That's what Zuckerberg wants." And all the big tech companies want clarity.

A few minutes later, someone from the audience returned to the subject, suggesting that we adults may care about privacy, but kids don't seem to care so much. Amoroso quickly jumped in. AI should make all of our decisions for us, he said with a grin. It should choose who we marry. Why not? We're already turning over our entire lives to social media.

His comment made Hackett think of another book: "The Inevitable," by Kevin Kelly, which says in one passage, echoing many Silicon Valley techies, that privacy as we know it is dead. Hackett doesn't believe that's true.

Nor does he believe that robots will take his job (another question from the audience). The future may well be automated. Former Google CEO Eric Schmidt came to Columbia Journalism School, where Hackett earned a master's degree, and delivered a talk on this, Hackett recalled. "It's coming, whether

we want it or not," was the gist. But of one thing Hackett remains convinced: Even if robots automate the mundane tasks, the world will still need journalists asking questions.

LEARNING TO CONNECT WITH CISOS

The next speaker confirmed that Amoroso has no interest in conventional conferences. He brought Rich Powell up on stage. Powell is TAG Cyber's lead illustrator. His best-known work appeared in Mad Magazine. He now draws a regular strip, in collaboration with Amoroso, called Charlie CISO. Not only does the comic appear weekly on TAG's website, companies can hire the two to create personalized strips to raise security awareness. A large cardboard cutout of Charlie CISO himself was standing nearby, in case anyone wanted a selfie.

"Did you ever think you'd be making jokes about cyber security?" Amoroso asked Powell.

"I didn't know what cyber security was," he replied.

After a few more questions about his career, Amoroso asked Powell if he had any ideas for their next strip. Remembering Amoroso's comment about AI during his talk with Hackett, Powell shot back: "Yeah, I thought we'd have AI pick someone's wife." He paused for a beat. "And it picks his mother."

After lunch, Amoroso stepped back onto the stage, alone this time. His keynote pulled together some of the ideas he'd promised. And though they weren't directly about commerce, they were ideas that could be used to produce it.

Alexander had already suggested some: Invest in people. Start with a large vision that can solve a problem. Listen to your employees. Hackett had touched on one at the end of his turn. Automation may change the workplace, but it's not going to eliminate a need for journalists—for people who can explain what's happening.

But Amoroso didn't start there. He started out talking about uncertainty, about the lack of solidarity, about "pathetic" state and local budgets. He spoke of the difficulty he'd encountered trying to teach a group of young people how to be executives. They were being groomed for management, just below the level of CISOs, but without any training.

Slowly he approached his subject: leadership. How do you lead? Why do people follow? Vendors struggle with this, he said. Nobody buys what you sell. They buy what you believe. "They buy into *you*." He challenged his audience: Sit in front of a mirror and deliver a pitch for your business without mentioning your product.

It was at this point that he brought up CISOs, who are often the professionals the vendors are pitching. (And presumably that's the reason Charlie CISO exists.) Stop thinking that there's a need that CISOs have that your product solves, he said. Even if it's true. "The reason you will make a deal," he continued, "is your ability to connect, not the quality of your product."

He finished his talk with three tips.

- Figure out who the people are you're trying to sell to.
- Don't choose tools because someone tells you to. Figure out the answer for yourself.
- And if you're a CISO, you need to decide whether you're also an executive. If you're not, you may need to take on a different role to make yourself well-rounded. But if all you want to do is hunker down and work on your SOC, you're not an executive. You're a hired gun.

INTERVIEWS

AN INTERVIEW WITH WITH SAL STOLFO, FOUNDER AND CTO, ALLURE SECURITY

PREVENTING PHISHING AND WEBSITE SPOOFING

The World Wide Web is the information superhighway that allows individuals and organizations to consume and share vast amounts of information quickly and efficiency. But as with any open entity, it can be used for harm just as easily as it can be used for good. As the web has grown, and as more content is readily available every day, adversaries understand the opportunities to create fake and malicious websites that can cause brand damage, financial harm, data theft, disruption, and more to legitimate businesses.

While the above are top-line business risks, it is tricky and time consuming for any organization to continuously chase down website-based threats. Allure Security provides a SaaS-based detection and takedown engine to help businesses prevent website spoofing and brand damage. We sat down with Professor Sal Stolfo, Founder and CTO at Allure, to talk about why spoofing and external website attacks have grown in prevalence in recent years.

TAG Cyber: What are some of the factors that have caused a rise in website spoofing attacks over the past few years?

ALLURE: Web spoofing and phishing attacks aren't new—they've been around for at least 25 years—with some of the earliest phishing campaigns targeting AOL users in an attempt to steal their login credentials. Phishing has always relied on the human factor—that's one aspect of the problem that is likely to never change. However, we have seen a dramatic rise in phishing attacks over the last 3 years, starting around the middle of 2017; there are several factors that have contributed to this rapid growth in the attack vector.

To understand the reasons phishing is on the rise, we should first take a step back and consider the motivation for phishers and other cyber attackers who target the general public. Simply put, it's all about the money. These criminals have built systems and supply chains to steal data and then monetize that stolen data. There are many classes of data that are attractive to these criminals. However, they all share a common bond: the data can be easily monetized. This data includes usernames and passwords for services like online banking, online gaming, online brokerages and insurance companies, as well as credit card numbers and other personally identifiable information.

Once a fraudster has their hands on a valid username/password combination, they will simply login and either directly transfer funds (ACH fraud) or collect personal information (that can be used for identity theft), or make purchases using saved credit cards (payments fraud). There is a multi-

billion-dollar industry in online fraud. And like any industry, one must continuously create (or collect) product to monetize.

With that backdrop in mind, there are technical factors that have driven the massive increase in phishing attacks over the last three years. The first are significant improvements in the security of websites and the infrastructure to support them. With modern cloud-based web firewalls deployed nearly everywhere today, it has become extremely difficult for an attacker to compromise a website to gain access to the large pool of customer data that sits behind it. The days of the giant data breach aren't over, but those events have become rare. Another significant factor is the effectiveness and ubiquity of endpoint antivirus software. Nearly every PC has some kind of AV installed and auto-updated, which has made it extremely difficult to execute mass-market malware attacks that steal data directly from users' machines. The third critical factor that has driven fraudsters to phishing is the emergence of bot management services. These bot management services are now widely deployed and have made it extremely difficult for large botnets to effectively brute force attack websites with large username/password lists.

These three developments have forced cybercriminals to change tactics. They can't break into the database of user data directly. They can't break into the users' machines. And they can't test massive data sets using automated bots. The highly technical attacks have been addressed with technical solutions. This has forced attackers to turn to social engineering and the human factor to get their hands on valuable data— and the only effective way to do that at scale is via phishing.

Recent events have made matters worse. With the fear and confusion arising from the global COVID-19 pandemic, and the various responses and support programs governments around the world have enacted, phishers have seen an opportunity to capitalize. It's been easy pickings for the phishers as they target the scared and vulnerable.

Automation has also made the cost negligible and deployment of phishing campaigns remarkably easy. Phishers have developed (and share) tools for spoofing legitimate webpages and for rapidly setting up and moving phishing sites to avoid detection.

Phishing has become a perfect storm of means, motive and opportunity.

TAG Cyber: Past methods for detecting spoofed sites have relied on domain registration monitoring and web searches. Why are these insufficient? How do they give attackers the upper hand?

ALLURE: In the past, most phishing websites typosquatted on a domain that can easily be mistaken for the real website address.

Typical techniques involve swapping an "i" or a "1" for an "l" or using the letters "rn" instead of "m." A site like www.alluresecurity.com can easily be mistaken for the real www.alluresecurity.com (can you tell the difference? Hint, upper case "i" looks a lot like lower case "L"). This technique is great for fooling the humans but can easily be detected with software that monitors domain registrations. For years, companies have been using domain monitoring software for just this purpose. But that's no secret to attackers.

To evade detection, attackers have avoided setting up typosquatting domains for their phishing sites, preferring instead to host the site on a domain with an unrelated name (or one distant enough that typosquatting detection won't find it). With more than 100,000 new domains registered each day, this allows attackers to hide their phishing sites among the millions of new sites that go up every month. Domain monitoring solutions lack the ability to continuously monitor the content on these new domains and determine if it is safe or malicious.

Another, more sophisticated technique phishers have been using recently involves hosting their phishing attacks inside of a working, legitimate and well-reputed domain. The phishers search the internet for established websites that have security holes. They take advantage of those holes to take some control of the site, such that they can add additional pages (their attack pages) inside the working site. This technique bypasses the domain system altogether, obsoleting that legacy domain-based detection approach.

TAG Cyber: We don't often think of honeypots and deception when we think of website security; how does Allure use these two tactics to protect customers?

ALLURE: When we were first thinking about how to address phishing— especially attacks that target an organization's customers,—we realized we had to contend with three hard truths: 1. Anyone can put a website online with whatever content they want - there is no way to stop that. 2. Anyone can send invitations to visit their website—there is no way to stop that either. 3. People who visit a website are free to interact with that website and type their personal information into that website—there is no way to automatically stop that even if the domain is malicious.

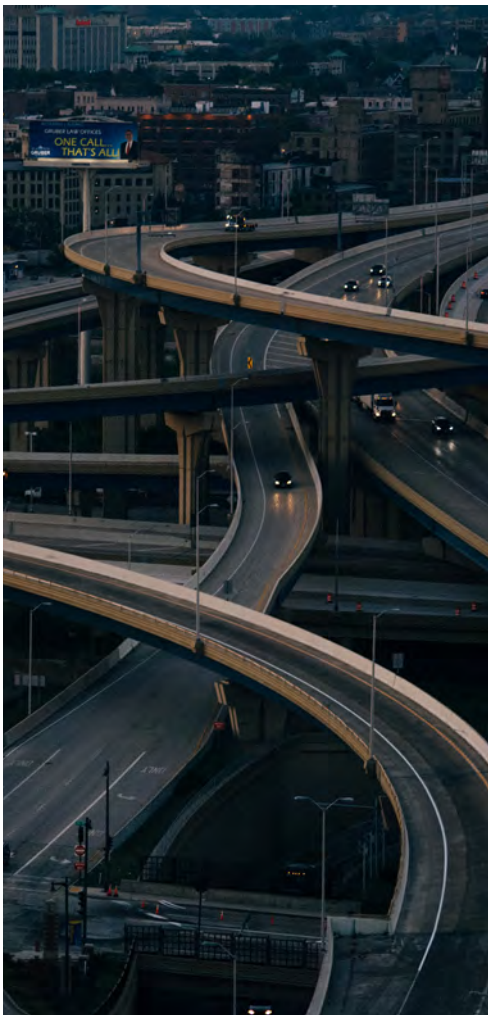
Simply put, it's all about the money. These criminals have built systems and supply chains to steal data and then monetize that stolen data.

We knew we needed to accept the truth but still wanted to find an approach that would put an end to phishing. What we came up with was to use artificial intelligence to create phishing victims, which then allowed us to turn the phishing campaigns into a honeypot for the phishers.

Here's how it works. When we spot a phishing attack, we analyze the site to determine what content the attack is after. Let's take the most common example, where the phisher's goal is to collect

usernames and passwords for a banking website. Our software sees that the site is asking for username and password data. We then instruct our deception system to generate a unique set of highly realistic decoy credentials and inject them into the phishing campaign, just like a victim would.

Using his technique, we are able to quickly poison the catch for the phisher, ensuring that the vast majority of data collected by their campaign are decoys provided by Allure. These decoys can't be differentiated from legitimate victim data that may have been collected. This leaves the attacker with data they cannot monetize— but it also sets a trap, the honeypot we mentioned earlier. If an attacker attempts to use Allure decoys, they are immediately detected, because the data is unique to the attack campaign and can be instantly identified. This allows us to profile the attacker and collect threat intelligence as evidence for attribution and potential prosecution.



TAG Cyber: What are some of the secondary or tertiary attacks companies can prevent if they stop attackers at the web level?

ALLURE: An organization that can protect their websites and other digital assets from being abused by attackers has an enormous business advantage over their competitors as well as over the cyber criminals. Endpoint-based activities almost always occur at the beginning of an attack campaign. Rapidly detecting and disrupting them prevents the downstream attacks they are designed to enable.

The most common downstream attacks are Account Takeover (ATO) and privilege escalation. These are the typical results of phishing, where the attacker steals credentials they will use to login to a system as someone else. What they do from there depends on the system, but this can easily lead to a customer's assets being stolen or internal IT systems being compromised due to loss of an administrator account (as we recently saw in the highly publicized Twitter breach). Other downstream threats include brand damage due to loss of customer confidence, losses of corporate data when successful penetration of corporate networks occurs, and losses of customers via accelerated attrition.

Ultimately, companies will be held responsible for losing customer data. Today it is primarily by the customers themselves, churning when their data has been stolen. In the future, it is likely to be driven by regulations such as GDPR, which imposes large penalties on an enterprise for a data breach. Now is the right time for enterprises to be taking action to protect their customers from the next generation of phishing threats.

AN INTERVIEW WITH WITH DAVID CHARTIER, CEO, ARCTIC SECURITY

AUTOMATED VICTIM NOTIFICATION TO REDUCE COMPROMISE

Despite the plethora of security and network monitoring tools deployed on the average organization's networks, the majority of large-scale breaches continue to be discovered by third parties—law enforcement agencies, researchers, or partners. The reason for this is that the complexity and difficulty of measuring and managing that attack surface isn't always straight forward. The number of interconnected systems, endpoints, users, devices, ephemeral networking environments, and so on is always expanding, making it hard for traditional security controls to keep up.

In a perfect world, security teams would have advanced warning systems, similar to a tornado warning system—but with greater time to react. This capability would allow organizations to know with relative certainty that they've been compromised and thus act immediately, driving down time to remediate, and limiting damage to networked assets and resources. This is exactly what Arctic Security has endeavored to build. David Chartier, CEO, of Arctic Security, spoke with TAG Cyber recently about victim notification.

TAG Cyber: How did you come up with the idea of an "early warning system" for cyber security?

ARCTIC SECURITY: The security industry puts a lot of focus on threat actors and predicting what they may be capable of doing and why. Whilst at the same time, millions of systems are already at risk because they contain vulnerable and misconfigured services or have already been compromised by malware.

We believed this problem was fixable and wanted to provide an effective way to notify the owners of those systems about the risks in their networks before bad actors had an opportunity to exploit the vulnerabilities or to leverage already gained access for lateral movement or further attacks. This breach information is essential for an organization to have in a timely manner.

TAG Cyber: In Cyber security, we talk a lot about "identify, detect, respond," but Arctic Security's message is automated victim notification. What's the difference, and why notification rather than identify or detect?

ARCTIC SECURITY: Our platform focuses on notifying customers about issues that can be seen on their networks already. The malware or the vulnerability is observable from outside and the customer needs to be notified as soon as possible so that they have more time to remediate. In doing so, Arctic Security makes the identification and detection activities of multiple independent researchers and sources easily accessible to end customers. These sightings often have been missed by the customers' other systems, including other technologies designed specifically alert on a potential security event.

But in the real world, where there is a cyber security talent shortage, budgetary pressures, and resource allocation considerations, there is no time to address every anomaly or potential threat—and companies need to focus their precious cyber security resources.

TAG Cyber: How does it work? Why don't you consider your technology threat intelligence?

ARCTIC SECURITY: Our platform automatically harvests a vast amount of threat data from over 100 different sources, including the customer's SIEM, threat intelligence feeds, sensors, incident response platform, and ticketing systems. It then normalizes and enriches that data, then matches it to the customer's specific networks, notifying them in real time about high priority issues needing remediation.

The reason we don't consider our platform threat intelligence is because the term "threat intelligence" is often understood to be something requiring a threat analyst to interpret and work on before any action can be taken. Our automated notifications of known and exposed vulnerabilities and already compromised machines are ready for remediation by the customer without any expert or analyst intervention. These issues can then be fixed by their IT staff.

TAG Cyber: Wouldn't it be better for companies to know everything, every anomaly, in their networks?

ARCTIC SECURITY: In an ideal world with limitless time and resources to address every anomaly, perhaps yes. But in the real world, where there is a cyber security talent shortage, budgetary pressures, and resource allocation considerations, there is no time to address every anomaly or potential threat—and companies need to focus their precious cyber security resources. Because the malware and vulnerabilities notified by Arctic Security are visible on the customer's network from the internet, that already makes them a high priority to address before a bad actor has time to exploit them. This targeted approach reduces false positives and removes the risk of alert fatigue, sadly so common in the security profession.

TAG Cyber: What are the biggest problem areas for your clients? (i.e., is it malware analysis, infected machines, etc.)

ARCTIC SECURITY: All of the above; the biggest problem is not realizing, until it is too late, that they have machines on the internet that have exposed vulnerabilities or have been compromised by malware. This problem is solved by our automated victim notification service.

AN INTERVIEW WITH WITH TUSHAR KOTHARI, CEO, ATTIVO NETWORKS

PREVENT LATERAL MOVEMENT WITH DECEPTION AT THE ENDPOINT

Deception has long been a valuable tool in thwarting would-be attackers. In the case of cyber security, deception technology lures adversaries away from valuable assets by presenting as juicy morsels—a production system containing sensitive data, a file filled with PII or IP, an admin account with high levels of access. The keys to deception technology are realism, creating an attractive target with which attackers will engage, and the ability for enterprise security teams to react in real time, preventing further propagation of an attack.

Attivo Networks has been a leader in the deception space, offering deception technology focused on in-network threats and endpoint attacks. As deception has become a must-have for enterprises, Attivo has evolved its offerings to cover cloud and provide analysis and forensics capabilities. We spoke with Tushar Kothari, CEO of Attivo Networks, about the current threat landscape and the role deception plays in organizations' defense strategies.

TAG Cyber: What are some of the more concerning attack trends you see?

ATTIVO: There are a number. First and foremost, ransomware threat actors are getting more aggressive and destructive. They have adopted so-called human-controlled ransomware and rely on APT-like techniques to move laterally and find critical data to encrypt. Organizations suddenly find themselves at the mercy of attackers encrypting their crown jewels or Active Directory servers and demanding exorbitantly high ransom amounts. These threat actors will often use information disclosure as leverage to force companies to pay the ransom. Second, attackers are more aggressively targeting Active Directory. Today's threat actors seldom scan the network when simple queries to AD will give them entire maps of the environment, whether they are looking for critical servers or administrative accounts. AD is so critical to regular operations that any disruption can be catastrophic. The data attackers can pull from an AD controller gives them the literal keys to the network. And next, credential-based attacks are increasing and attackers have used credential theft in over 65% of incidents last year. While Ransomware 2.0 may be responsible for some of this increase, attackers leverage stolen credentials to elevate privileges, infiltrate the network, and steal data. With stolen credentials, attackers don't need to exploit services; they can just log into a server from a compromised endpoint and move around. It's now more critical than ever to prevent an attacker from moving laterally off an endpoint. Organizations need to comprehensively be able to detect threats across all attack surfaces and vectors to find and stop lateral movement activity.

With the transition to a remote worker environment, there are concerns around cloud attacks and remote work security. Attackers can target remote workers for cloud or VPN credentials to gain entry into the network. Protecting the cloud environment is a challenge in and of itself, as demonstrated by multiple compromises traced back to misconfigured cloud environments.

Finally, attackers are targeting non-standard infrastructure like IoT to gain access to the organization. IoT devices have vulnerabilities that organizations can't patch and often exist on the same networks as production systems and servers despite best practices to the contrary. Attackers will target IoT devices because security is usually not part of their design, making them easy targets for compromise and a pivot point into the rest of the network.

TAG Cyber: A big theme for Attivo has been "enhancement." You've announced several partnerships with other leading security vendors. Why is the idea of enhancement important?

ATTIVO: There isn't any silver bullet in security and organizations need a layered defense to reduce risk and secure their data. They can also greatly benefit from tools working together to share information and automate attack analysis and incident response. For example, for endpoint protection, EPP and EDR solutions are each designed to do specific things. EPP provides capabilities such as automated patch management, maintaining devices remotely, and protecting endpoints from attacks. Alternatively, EDR uses behavioral detection techniques to examine process flows and chains to see if something looks unusual, and then responds to the attack using collected IOCs and forensics.

Each is valuable and effective in what it does. However, alone they do not offer comprehensive detection for all methods of attack, especially when it comes to lateral movement detection. This is a core competency of the Attivo Endpoint Detection Net (EDN) solution, which has demonstrated using the MITRE ATT&CK assessment DIY tools to improve endpoint detection by an average of 42% when used with an EDR solution.

TAG Cyber: Attivo recently published research citing endpoints as a top security concern. This jives with other industry data about the prevalence of endpoint-focused attacks. How does deception at the endpoint work differently from in-network deception?

ATTIVO: In-network deception refers to decoys that look like production systems and act as engagement servers for attackers. These decoys record forensic data of all attacker activity that occurs at the disk, memory, and network layers. Endpoint deception deploys on production systems to derail lateral movement by leading attackers to the network decoys.

Today's threat actors seldom scan the network when simple queries to AD will give them entire maps of the environment, whether they are looking for critical servers or administrative accounts.

These deceptions consist of fake credentials, bait files, hidden mapped shares that lead to decoy file servers, and Active Directory deceptions that return false information to unauthorized queries pointing to the engagement environment. They can also conceal local files, folders, removable storage, production mapped network shares, and even cloud storage so that attackers and malware, such as ransomware, can neither see nor access them, limiting damage to production data and only showing deceptive assets for engagement.

The Endpoint Detection Net Suite (EDN) is specifically focused on preventing the attacker from moving laterally from an endpoint. We looked at various attack methods used by attackers to break out from the endpoint and created a variety of lures, mis-directions, and decoys designed to derail the attack. These include the capability to detect credentials theft, man-in-the-middle attacks, unauthorized queries to AD, discovery of network assets, attempted compromise of file servers, exploitation of services, as well as visibility to the attack paths an attacker would use to reach their target.

These detection capabilities augment and close gaps from EDR solutions, reducing risk and dramatically reducing dwell time. Additionally, data from these alerts can be shared through native integrations and be used to automate the isolation of an infected endpoint, which can be extremely valuable in shutting down ransomware or other destructive attacks.

TAG Cyber: How has the increase in remote/home-based work changed how organizations need to protect themselves, and what role does deception technology have in that plan?

ATTIVO: The sudden move to a predominantly remote work environment forced organizations to expand their VPN access and cloud services infrastructure rapidly. In the race to get as many people as possible working remotely, companies did not have time to consider how these changes could affect their security controls. Their firewalls, proxies, IDPS, and other network perimeter security controls don't offer the same level of protection to remote workers, especially when they configure split tunneling to segregate business traffic from personal traffic. An attacker can compromise a home user with VPN access and gain entry into the network. Activity baselines are no longer accurate, and investigations become more complicated, as most of the network traffic originates from the VPN segments. User credentials for cloud, SaaS, IaaS, and VPN access become critical to protect since any compromise gives threat actors access to essential data.

Deception technology can mitigate many of these concerns. It can monitor VPN, cloud, SaaS, and IaaS credentials for unauthorized use or theft. Decoys within the VPN segments and

cloud infrastructure can detect discovery activity on the network and in Active Directory. They can identify compromised systems that attempt lateral movement activities from within the VPN network segment and augment existing security controls with visibility and detection.

TAG Cyber: What are some misconceptions about deploying deception technology?

ATTIVO: Deception has to be one of the most misunderstood security technologies on the market. Some of this derives from legacy associations with honeypots, which provide limited research value and where adoption was hampered given its complexity to deploy, operate, and manage. A modern cyber deception platform is materially different from a honeypot in several ways. First is the depth of deception. Today's deception technology is designed for scalable detection across on-premises, cloud, and remote locations, which means that it must be easy to deploy and operate. The use of machine learning has turned what used to require highly-skilled workers and ongoing tuning into a fully automated environment that is now tuned for ease of deployment and scalability, as well as optimum authenticity.

Cyber deception also now goes beyond the use of decoys and provides deception lures, bait, and methods of derailment that anticipate how an attacker attacks and hides real credentials amongst deceptive ones that breadcrumb the attacker to a decoy. Additionally, the ability to hide Active Directory and files, folders, removable drives, and mapped shares make it exponentially more difficult for an attacker to find a target, no less compromise it. The last common misconception is simply whether it works. With today's deception using high-interaction real OS and applications as well as other advanced deception designed to derail APTs, it has consistently proven itself during red team testing and security assessments to detect and record attacks with precision.

AN INTERVIEW WITH WITH MICHAEL CUTLIP, ADVISOR TO THE BOARD OF DIRECTORS, AUTHORITI

ELIMINATE FRICTION AND FRAUD WITH SMART PINS

Businesses and individuals transact every day—from authorizing payments for goods and services rendered, to permitting healthcare providers to share health records, or for allowing a mortgage lender to ensure payments are routed to the right account.

The importance of "getting it right" cannot be overstated. We've all heard the story in which a "CEO" instructs a finance employee to wire $10,000,000 to an overseas bank account. Immediately! The finance employee does as they're told, because the instruction came from the CEO. It turns out, though, that the "CEO" was a fraudster posing as the CEO and the bank account is that of some cybercriminal.

Scams targeting vendor payments, banking transactions, healthcare real estate, and more are on the rise, facilitated by business email compromise, and the Authoriti Network offers a client-side application that puts control over transactions back into the hands of authorized parties, helping prevent fraud and identity theft by eliminating the potential for misuse. We spoke with Michael Cutlip, Advisor to the Board of Directors at Authoriti, about their innovative authorization technology.

TAG Cyber: Today, there are many technologies focused on authentication, but fewer focused on authorization. Why do you think that is?

AUTHORITI: There are a few reasons. First, authentication has been pressured by bad actors and forced to improve. However, the enhancements have evolved a legacy model rather than fundamentally change it. The legacy centralized challenge/response security model is ancient. "Halt, who goes there?" generally worked because the individual with the password then immediately transacted in person and in the moment.

Challenging digital users at the other end of the line to prove who they are is a simple extension. Security measures have been layered to improve authentication when the prior method was deemed ineffective. This includes: Knowledge Based Authentication (KBAs), centralized One-Time PINs (OTPs), and backend monitoring/analytics. Multi-factor authentication, to which you referred, is just a combination of these many ways to authenticate.

The second reason is that authorization is largely confused with centralized access control. It is a process that hasn't had seen the same level of criminal pressure, and thus sits in the "necessary-but-boring" bucket. Nonetheless, it's vital. For example, based on early reports, the takeover of multiple Twitter accounts in July appears to have been related to insufficient access controls.

TAG Cyber: Why is the authorization piece important?

AUTHORITI: Fraud is a bad transaction, not a bad person. Authenticating "who" is on the other end of the line is only one part of the puzzle; it's the

The legacy centralized challenge/ response security model is ancient. "Halt, who goes there?" generally worked because the individual with the password then immediately transacted in person and in the moment.

action that person takes ("what" they do) which causes a loss. It is therefore vital to ensure that the transaction request was authorized by the authenticated customer or employee. You can't stop at authentication.

Further, it's important to note that most digital authentication procedures are dependent on an in-the-moment basis. They maintain connection to the central server to hold trust in the identity. However, there are many scenarios where that channel is either not available or should not be trusted. Redirecting the genuine transaction of an authenticated user can have the same negative impact as stealing and misusing an ID.

TAG Cyber: Can you describe some of the trade-offs between security, access, and ease of use?

AUTHORITI: The classic trade-off between risk management and user experience was typically won by the risk side; a little inconvenience was necessary to manage fraud and protect private data. Customers were simply happy to be able to transact online and accepted the friction as evidence that the company was looking out for them.

Over time, after those layers of protection broke customer experience, the system was ripe for change. The customer-first focus and new technology platforms that startups have brought to every industry has radically shifted the balance toward UX. That said, some of these new customer-friendly technologies appear to have allowed fraud levels to rise, in part because they are still built around centralized authentication.

Focusing on data privacy issues, companies holding central stores of customer and employee data have long tried to protect it, given the clear liability issue for the holder. Consumers, however, are only now becoming aware of the extent to which their data is being collected and used by enterprises, having earlier consented via dense legalese in order to use the convenient or fun new services.

Rising consumer awareness and regulatory oversight is mandating that companies (data holders) provide an easy and clear control mechanism for consumers (data owners) to provide or withhold consent on how their data can be tracked and processed (used). Finding solutions that allow companies to easily eliminate friction and fraud while improving data privacy is everyone's goal.

TAG Cyber: How does the Permission Code® platform reduce customer friction and mitigate fraud risk?

AUTHORITI: Authoriti's mobile-first platform gives users control to authorize any transaction when and where they choose. Users do not have to be constantly connected with the other party to

transact. Bridging that time gap between authentication and execution allows Authoriti to eliminate a large source of friction. Further, users no longer must respond to challenge questions (criminals already found the answers online anyway) or wade through an IVR maze (the ultimate in annoying) or wait for and then return a simple Dumb PIN (which criminals intercept and misuse) just to prove who they are. Finally, the weaknesses in traditional authentication has led to transaction monitoring. These

backend platforms are educated best guesses which still generate a significant number of false positives (again, risk wins out to reduce losses), resulting in frozen transactions pending investigation (also known as friction).

With Authoriti, users generate secure content-rich Smart PINs which confirm both their identity and details of the transaction they're authorizing the recipient to execute. Because the Smart PINs are restricted to a specific transaction, and are encrypted and digitally signed at creation, they are tamper-proof and can be distributed through any channel without the risk of interception and misuse. That's important for the future as channel security becomes complicated by intermediaries such as chatbots or intelligent assistants. Parties receiving a transaction request with a Permission Code® PIN can easily validate the instruction through a simple API call to Authoriti and then immediately execute with confidence because the PIN provides a definitive record.

We touched on data privacy earlier' one interesting feature of our Smart PIN is its ability to evidence delegation of a user's authorization to a third party. Since the user is creating the Smart PIN, they can embed a third party's identification in the PIN. This enables an easy mechanism for data owners granting consent for a data holder to share data with another party for processing (e.g., data aggregation).

TAG Cyber: Where do you see PII privacy headed in the coming years?

AUTHORITI: Regulations controlling PII will become more and more strict, resulting from growing consumer concerns about data harvesting by social networks, and likely expanding in reach beyond just PII. We see a day when we focus as much on how accounts and transactions are processed as we do today on checking identity. Consumers, regulators, and businesses all share a common goal of eliminating the misuse of all information.

AN INTERVIEW WITH WITH RAHUL KASHYAP, CEO, AWAKE

YOUR NETWORKS ARE YOUR GROUND TRUTH

Network analysis is one of the most important things companies can do. The ability to determine good from bad, normal from anomalous, and permitted from unauthorized is more important than ever, especially given that "the network" can be a traditional, on-premises data center, and it can encompass cloud and virtual environments, containers, and the interfaces between partner and supplier networks. The use of off-premises environments doesn't obviate the need for traffic analysis. In fact, some might argue that the need for complete visibility and a thorough understanding of traffic patterns and behaviors is even more critical in third party-controlled environments.

Wherever your company's applications and services are communicating, the network is the "ground truth." But it's not just layers 3 and 4 of the OSI model that are important today. To properly manage the network, you need to analyze network communication at layers 2-7, plus the ability to investigate and remediate issues. Awake Security is built on this very premise but goes beyond basic network packet capture. We spoke with Rahul Kashyap, CEO at Awake. about this important space.

TAG Cyber: In your work with enterprises, what are some of the common misperceptions about the "network"?

AWAKE: Let me start with a stat: We find the average organization is aware of between 40-50% of what is on their network. And of course, if you cannot see it, you certainly cannot protect it. These unmanaged devices have no endpoint security agent, no logs being extracted, etc. In other words, they go unmonitored by the security team.

The other aspect is the unmanaged infrastructure is more than just BYO and shadow IT devices. It is often the stuff that's hiding in plain sight. For instance, the TVs and phones in the conference rooms are all IP enabled, so are your thermostats and security cameras. Similarly, people tend to forget the contractors and other third parties that connect to their network.

One other misconception I hear is that network security is dead, even in the context of this new network. Why? Because so much data is encrypted. I think this is clearly a case of the security industry having dropped the ball and given up. With advances in data science, it is possible to draw meaningful security inferences even if that data is encrypted. We need to innovate our way through these challenges not simply throw in the towel.

TAG Cyber: Why does the definition of "network" matter?

Awake: It comes down to the fact that each unmanaged device presents a vector into your environment. We see multiple successful breaches that start with the unpatched and often exposed infrastructure and then make their way into the rest of the environment.

Let me put this into context. Many organizations today have their data crown jewels sitting in a SaaS application accessed through the browser. In June 2020, we disclosed a massive browser-based surveillance campaign that targeted millions of users across a wide variety of enterprises to steal sensitive data including application credentials, keystrokes etc. The browser extensions that enabled this attack easily evaded endpoint detection and response solutions. They also activated themselves, often on personal devices with the same browser access, to the SaaS application but without any real security controls. If you don't know these personal devices are accessing your data, how do you protect that data when the devices are compromised?

TAG Cyber: How can companies calculate risk when threats are changing daily?

AWAKE: Risk is a bit of a loaded team in security. Unfortunately, it has become synonymous with the notion of an alert being high, medium, or low. This is a very rudimentary approach since you have very little context about the entity involved in the alert—is this the device that displays the menu in the cafeteria each morning or is this your CFO's computer?

Our recommendation is to take an asset-centric, continuous observation perspective to risk. In other words, you monitor a device, user, or application; you know who or what the entity represents; and over time, you can track its behaviors, looking for even weak signals that indicate an impending threat. Having that historical perspective allows you to optimize the security operations workflow, starting with devices or users that mean something in the real world vs. an abstract alert.

Let me give you an example of why context is important to the risk calculation. Ransomware, in most cases, is detected once your data is in the process of being encrypted and/or exfiltrated. Clearly yes, it is high risk at this point, but it is also perhaps too late to make that assessment. On the other hand, taking this entity risk posture can bubble up risky behaviors that are early warning signs of a ransomware threat—something that ordinarily is easily ignored is now a high-risk warning of a potentially devastating attack.

TAG Cyber: How does Awake's platform handle the proliferation in unmanaged devices communicating on enterprise networks?

AWAKE: First, it's worth mentioning that almost every threat manifests on the network. It is also very hard for the attacker to hide their traces on the network—there is no unsending a packet like you might delete logs or uninstall or cripple an endpoint security agent. So, our first approach was to start with ground

truth data. We take that data collected and parse the entire communication, from layer 2 on up.

Why do this as opposed to relying on a threat signature or parsing protocols like Kerberos

or SMB, for instance? Because it provides a great mechanism for discovering unmanaged infrastructure and then monitoring it. We use this activity and entity information to construct a security knowledge graph that we call EntityIQ. Now we can track this entity based on a behavioral fingerprint—whether managed or not. In fact, this fingerprint allows us to track the entity as it moves across the organization, even if IP addresses change or the device jumps on a different network. And then as I mentioned earlier, we can track risk at this entity level.

TAG Cyber: What role does modeling play in your solution?

AWAKE: One of the things we observed in the market was a bunch of AI-based solutions that, simply put, were black boxes. There was no explanation about why something became an alert. Kind of a "just trust the AI" approach. We wanted a more refined approach making the AI fully explainable. To do that we built an adversarial modeling language (AML)—a vocabulary to describe behaviors. Using this vocabulary allows the detection of the tactics, techniques, and procedures used by an attacker rather than a specific point-in-time domain or malware hash.

A portion of our detection logic is built using AML. It is included in the product transparently. Customers can use as is, adapt, modify, or even build their own logic and share with peers. Now, when a model fires, customers have all the behavioral details, along with a forensic timeline, about the entity's behavior.

There is one more benefit: We provide a point-and -click model builder that many of our customers will use to threat hunt. The model can easily be saved for future automated detection. For instance, one of our customers is a consumer finance giant. They built a custom model using AML which monitored individual users who were leaving the organization. The model looked for large 'from' SaaS applications like Microsoft 365 and 'to' personal cloud storage systems like Google Drive. This customer took a human resources process and added a monitoring control with little friction.

With advances in data science, it is possible to draw meaningful security inferences even if that data is encrypted.

TAG Cyber: What do you see as the difference between "automate" and "autonomous" in the context of security?

AWAKE: A good analogy is to compare cruise control with a full self-driving car. The former is automating the mundane task of pressing the accelerator while the latter is using a variety of sensors to autonomously control and navigate. The same can be

said of security. When people talk about automation, it is really about the mundane—automatically correlating data across a variety of security tools.

Autonomous security is a lot more interesting. It's about taking experience and skills and building them into a knowledge-based software system. For instance, when responding to a suspected phishing domain, there is a standard set of questions an experienced analyst asks: Who else visited that domain? What other domains are part of this same attack infrastructure? Who visited those other domains? Did we see any lateral movement from the compromised device? An autonomous security system asks these questions even if a relatively junior analyst doesn't know to ask them. The data is automatically pre-computed and presented to the analyst so they can focus on risk management decisions rather than data crunching. Leave that to the machines!

AN INTERVIEW WITH WITH DEAN SYSMAN, CEO AND CO-FOUNDER, AXONIUS

A HOLISTIC APPROACH TO ASSET MANAGEMENT

It goes without saying that keeping track of software and hardware assets in today's networking environments is a complicated task. Beyond what exists on the traditional on-premises network, companies now have to consider how to track and manage ephemeral cloud instances, virtual machines, IoT devices, mobile devices, other endpoint devices, and more. Gaining a comprehensive asset inventory in a continually changing environment is hard enough, but simple accounting isn't sufficient to protect systems, users, and data.

Dean Sysman, CEO and Co-Founder at Axonius, spoke with TAG Cyber about asset management, which starts with an always up-to-date inventory, but must go further to include the ability to see gaps in security coverage and allows for automation of policy validation and enforcement across users, systems, and environments.

TAG Cyber: Why do enterprises continue to be challenged by asset management? This isn't a new problem.

AXONIUS: Asset management is a core component of any security program, but many companies simply don't know exactly how many assets they have or what's on them. Today, enterprises have a lot of systems that know about assets, but they are siloed. The result is that asset inventories are never up to date, and because they aren't being updated continuously, there are many risks introduced. These can include newly provisioned devices without endpoints installed on them, a new cloud instance created that isn't being scanned for vulnerabilities, and more.

To have an effective asset management program, enterprises need a comprehensive asset inventory that is updated on a continuous basis. Without knowing everything you have, you can't effectively know that your security policies are being applied everywhere, and that you've assessed all the possible risk in your environment.

TAG Cyber: Can you talk a bit about the differences between managing traditional IT assets and IoT or OT assets?

AXONIUS: Many agents used as security controls to manage traditional IT assets cannot be applied for IoT and OT devices that require availability at all times. Furthermore, these devices may reside on special segments of a network that are zoned off from the IT network, making it complex and costly to account for them with network scanning-based controls. Additionally, cyclical scans will show devices they found during a scan, but what happens in between scans? This

A study…shows that comprehensive IT asset inventories take over two weeks of effort (89 person- hours of labor) and happen 19 times per year, on average

dynamic environment is a large reason why enterprises have a difficult time accounting for all IoT and OT devices they have.

Many of our customers are able to more easily discover and manage IoT and OT devices by simply connecting to all the systems that know about them rather than using a single agent or scanning-based approach. This allows them to discover all devices, while not sacrificing on visibility or availability of the devices themselves.

TAG Cyber: The average enterprise has more than 100 security technologies deployed across environments; why does this make asset management even more complex?

AXONIUS: Even with so many tools, organizations still report visibility gaps. Security complexity (threats, regulations, etc.) drives more siloed tools investment, further complicating the problem. This will become even more unmanageable unless we solve the first problem: understanding and managing what we have.

Today, asset inventories are overwhelmingly complicated! A study commissioned by ESG shows that comprehensive IT asset inventories take over two weeks of effort (89 person-hours of labor) and happen 19 times per year, on average, requiring multiple teams and people*. The rise of ephemeral devices, such as containers and virtual machines in the cloud, makes this challenge even harder. Ephemeral devices are used for a short period of time, and often forgotten and left unprotected.

To truly close visibility gaps and get a credible asset inventory, a new approach is needed.

TAG Cyber: Can you explain what an "adapter" is in Axonius' terms, and explain the benefit of this program?

Axonius: Adapters are pre-built integrations for the Axonius platform. Adapters gather and aggregate data on devices and users from the solutions you're already using, which means you can:

- Create an asset inventory for customers without scanning their network or installing agents on devices;
- Refer to as many sources as possible to understand the current state of an asset; and
- Understand whether the asset meets a risk control and adheres to a given security policy or framework.

Today, Axonius has over 200 adapters and we continue to add them based on customer demand.

** ESG eBook, 2020 Asset Management Trends: As IT Complexity Increases, Visibility Plummets, March 2020*

AN INTERVIEW WITH WITH MATT KEIL, DIRECTOR OF PRODUCT MARKETING, CEQUENCE

REDUCE THE RISK OF A SUCCESSFUL API ATTACK

When APIs started coming into use in the early 2000s, programmers couldn't have predicted just how critical to daily operations they would become. Today, heading into 2021, application programming interfaces (APIs) are the communications "glue" that holds together applications, components, microservices, and containerized workloads. Driven first by mobile device and cloud ubiquity, and now by DevOps with its modular development, organizations rely on hyper-connectivity to facilitate feature-rich user experience and business interoperability.

As APIs make software available to workloads and applications for bidirectional communications, message sharing, and memory sharing, their functionality is predicated on an open and available architecture. These same attributes also make them excellent targets for bad actors.

Cequence Security offers an application security platform that allows enterprise security teams to detect and mitigate API-based attacks. We spoke with Matt Keil, Director of Product Marketing at Cequence, about the API threat landscape and how organizations can implement preventative measures against attacks.

TAG Cyber: How are bad actors abusing the API ecosystem to execute attacks?

CEQUENCE: APIs are the plumbing by which data moves back and forth between applications. The highest risk APIs are those deployed outside of a defined process (Shadow APIs), those that do not adhere to a defined specification (non-conformant) and those that are old, or not end-of-lifed properly (deprecated). It's also critical to remember that APIs are stateless and include the entire transaction, such as the level of access control, which, if exposed, would allow an attacker to change permissions (via a parameter such as "admin=yes"), alter data (modify dates, times, dollar values) or steal data. As such, APIs are an attack vector that can result in data loss, fraud, or destruction, just as you might see in a more traditional database or web server vulnerability exploit.

TAG Cyber: How is the explosion in API usage impacting cyberattacks?

CEQUENCE: The beauty of using APIs is that you can build and deploy functionality and data integrations quickly. Those same benefits are leveraged by bad actors to achieve their end goal of stealing data or committing fraud. Shadow APIs, or those that do not follow their OpenAPI defined specification, might allow a bad actor to gain elevated privileges; they may expose too much information in an error message or response code that can then be used for the next phase of an attack. Finally, APIs make it easy to execute automated attacks— account takeovers, scraping, fake account creation, and other forms of abuse. It is far easier for a bad actor to script against an API that it is for them to script a form fill.

TAG Cyber: What are some of the most common attack types against APIs?

CEQUENCE: Currently, the most common form of API abuse is automated bot attacks such as account takeovers, scraping, and fake account creation. As more APIs are exposed to the public, bad actors are shifting their targets to the data that resides behind the APIs by abusing privilege settings within the API, looking for those APIs that have no authentication, or are sending sensitive data in plain text (no encryption). These types of errors are found most often in shadow APIs or those that may not follow a specification.

TAG Cyber: If the exploit of an API is the first foothold of an attack, what are the potential consequences?

CEQUENCE: There are numerous high profile examples of API-based attacks resulting in the exposure of user information, loss/theft of data, and automated attacks. Facebook, Panera Bread, Twitter, Uber, CapitalOne, and Samsung are just a few of the companies whose APIs have been exploited. In some cases, the attack result may have been achieved directly via an API. In other cases, the API was one of several phases in the attack. At the end of the day, an API is plumbing for the application. When an attack happens, the loss or the outcome is what makes the news. The fact that it is an API often times is not an area of focus.

TAG Cyber: How can organizations reduce the risk of a successful API attack?

CEQUENCE: There are three ways in which an organization can reduce their API security exposure. Number one, visibility: Organizations can reduce their API security exposure by first gaining a full understanding of their entire API footprint including deprecated, hidden, and shadow APIs published outside of security teams' visibility and left unprotected. Security best practices revolve around knowing what is on the network, where the traffic is going to and coming from, and what the payload might be. Armed with the knowledge of what APIs have been published, the security team can implement an appropriate policy. Outside of the standard firewall and threat protection policies, the API can be protected using geo-fencing to restrict traffic coming from known bad regions; or they can block owners (organizations) with known bad IP addresses.

APIs make it easy to execute automated attacks— account takeovers, scraping, fake account creation, and other forms of abuse.

Second is specification conformance: Organizations that are moving towards API-driven development methodology will often adopt an API specification framework like OpenAPI that helps guide API developers during their coding process. By definition, a shadow API is published outside of the process that may confirm it is following the specification. There are many examples where a specification validation may have avoided significant security

incidents again, Panera Bread, Uber, Twitter, and Facebook all come to mind. The benefits of using a specification as a guideline can find and eliminate potential security gaps that may result from unpublished and hidden API endpoints, headers, parameters, and response codes in use. Those elements that are discovered as non-conformant can be flagged and addressed by development. By adhering to the specification, critical elements such as access control, authentication, and encryption can be validated, thereby reducing the security exposure.

And number three, adhere to the defined API use case: An API, like any application, is created to achieve a goal, often called a use case or "story" in development language. Each use case should be documented and should address how access control, authentication and sensitive data is treated. They are as follows:

- Access control: stops a bad actor from gaining access to user information (to execute an account takeover), change permissions (via a parameter such as "admin=yes"), alter data (modify dates, times, dollar values). Ensuring that API access control is implemented properly can go a long way toward avoiding a security incident.
- Authentication: validates who you say you are via API keys, OAuth, or other mechanism. Unfortunately, authentication errors abound. In some cases, API endpoints are left unauthenticated (Panera Bread), in others the API keys are hard coded or exposed in the mobile app (Trump Campaign Mobile App). If API keys are used, following best practices will help you avoid a CLM: use them for read-only functions; avoid sending them as part of your query result in a URL. Best practices recommend inserting the API key in the authorization header. For higher value APIs, OAuth/OpenID or SAML should be used.
- Encryption and sensitive data: A recent report from the Palo Alto Unit 42 research team found that out of 1.2M IoT devices, which typically rely heavily on APIs, a staggering 98% of them did not use encryption. None. Given that API transactions will often include sensitive PCI or HIPAA data, encryption should be enabled by default.

AN INTERVIEW WITH WITH DEBBIE GORDON, FOUNDER AND CEO, CLOUD RANGE

SIMULATION TRAINING TO IMPROVE YOUR EMPLOYEES' SKILLS AND JOB SATISFACTION

Cyber attack simulation training using a cyber range has emerged in the last several years as an effective way for SOC analysts to practice defense against real-life cyber threats. In the past, SOC operators and incident responders were relegated to incident response exercises, product training and awareness, certification/classroom education, and instructor-led workshops or training. All of these exercises provide benefit, but none can fully prepare operators for a bona fide attack. Those traditional methods aren't enough to prepare SOC teams for the high pressure situations where every minute counts, and the lack of realism of a traditional incident response scenario often can't match what analysts experience during an actual attack.

Cloud Range, a cloud-based cyber range training company and platform, provides cyber range training just as other industries use simulation training. In aviation, pilots are required to complete a certain number of hours in simulated flight training before they're allowed to fly solo. Professional athletes use simulation to perfect their skills and better anticipate adversaries' actions on the playing field. Cyber security should be able to take advantage of the same type of training to prepare for adversarial attacks, too. We spoke with Debbie Gordon, CEO & Founder of Cloud Range, about attack simulation training and how it advances cyber security defense.

TAG Cyber: Please explain how cyber ranges differ from and complement traditional incident response exercises?

CLOUD RANGE: There are a few significant differences between traditional incident response exercises and simulation on a cyber range. Traditional exercises are imperative, but actual SOC simulation is another dimension of preparedness that has not existed until now. As the last line of defense, SOC analysts must develop knowledge, skills, abilities, and ultimately "muscle memory" by going through simulations frequently. Each exercise represents a unique type of attack scenario, and the more immersed they are, the more prepared they are, both individually and as a team. Traditional incident response exercises may only be done one or two times per year, and they typically focus on what to do once a situation has already become dire. Additionally, they are usually theoretical and don't involve simulation of the attack actually being detected, before it may become dire. Incorporating a virtual cyber range into a company's toolset can be the difference of preventing a breach before it actually happens and a devastating attack. Traditional simulations should still be conducted, but having cyber range simulations will significantly and measurably reduce a company's risk.

From a practical standpoint, true cyber preparedness by SOC analysts is rooted within a few different factors. While industry certifications and manufacturer product training are important, practical, hands-on

Without real-life experience, security teams need to wait for a real cyber attack to happen to determine if they know how to handle it

experience is often the missing part of that equation. Traditional training and certifications, as well as incident response exercises, are theoretical and don't provide a hands-on technical approach to simulating a cyber attack . Without real-life experience, security teams need to wait for a real cyber attack to happen to determine if they know how to handle it, but at that point, it is too late. Cloud Range provides a safe environment that can mimic an organization's infrastructure and security tools in order to provide the most realistic and immersive experience where failure is an option. With frequent exercises and a variety of attack scenarios, security teams gain the skills and ability to effectively detect, respond, and remediate a multitude of threats without putting their organization at risk.

Cloud Range provides security teams the opportunity to gain real-life experience and develop the skills needed to identify, defend, and remediate against cyber attacks. By regularly engaging in simulated cyber attacks in a live network environment, cyber defenders can then develop the muscle memory necessary to be able to react in a split second against any given threat.

TAG Cyber: How do you come up with realistic scenarios?

CLOUD RANGE: Cloud Range's Threat Intelligence Team is constantly studying the threat landscape including tactics, techniques, and methods that threat actors will employ to ensure our clients are staying ahead of impending threats. This is especially important with changes in trends and the global environment. Our content is all mapped to the MITRE ATT&CK framework. Additionally, our team designs scenarios based on business-specific and industry-specific vulnerabilities.

TAG Cyber: You've talked about dwell time a lot in the past. Is time the only measure of success in Cloud Range's simulation exercise?

CLOUD RANGE: By engaging in Cloud Range's simulation exercises, reducing overall dwell time is a measurable result that reflects an organization's risk levels, however it is not the only measure of success. A security team functions like a sports team where the whole is greater than the sum of its parts. Each person must be evaluated on knowledge, skills, and abilities as an individual to ensure that they are contributing to the success of the team, which is measured separately. Cloud Range has developed proprietary evaluation methods that show a very clear picture of how effective a security organization is. This maps directly to the NICE Framework, while ensuring that results are simple and valuable to the C-Suite.

Secondarily, given the severe cyber skills shortage, it is imperative that companies retain employees. Cloud Range customers have

a measurably higher chance of retaining their employees who participate in the simulation exercises, as it provides a greater sense of purpose and understanding, which leads to job satisfaction.

TAG Cyber: How has the hyper work-from-home environment changed the types of scenarios you may add to the offering?

CLOUD RANGE: With more analysts working from home, there are new dynamics introduced into incident detection, response, and remediation. Fortunately, our virtual cyber range was designed to provide simulation training to customers regardless of location, given the growth of distributed security teams over the last five years. By providing training remotely via video conference and RDP, our customers have benefited even more from our services because remote workforces require a new set of communication methods and processes over and above their technical skills. These are significant areas of focus— working with remote teams to ensure security skills and communication skills are developed and effectively implemented.

TAG Cyber: What are the types of benefits organizations can expect when they implement cyber range training?

CLOUD RANGE: Implementing regular cyber range simulation training gives every member of an organization's security team the ability to learn and practice defending against attack vectors in a safe environment. In addition to honing their skills using actual security tools, SOC teams and individuals will feel more engaged in a gamified environment that reflects the most current, real-world attack scenarios. This type of gamified, realistic, hands-on training and exercises can lead to higher employee satisfaction and retention.

By incorporating cyber range training into their cyber defense regimen, SOC teams can also track their progress using metrics that reflect actual detection and response times for each team member. Being able to measure a team's cyber preparedness using real data will inspire confidence in their abilities to detect, respond to, and remediate against virtually any cyber attack that may occur.

AN INTERVIEW WITH WITH RAJ MALLEMPATI, CHIEF OPERATING OFFICER, CLOUDKNOX

ENABLING CONTINUOUS SECURITY ENFORCEMENT IN THE CLOUD

The accelerating transition to hybrid and multi-cloud environments creates awesome opportunities for enterprise teams to deliver new services, reduce operating costs, and optimize their ability to delight customers. The corresponding cyber security challenges, however, continue to influence the risk equation, which can slow down the benefits of adopting cloud services and infrastructure.

One of the most important elements in this risk equation involves securing multiple cloud platforms in the context of the permissions, and roles for identities and resources that must be managed. Insider threats, in particular, represent a particular challenge— one that is best addressed by ensuring least privilege implementation across all cloud services. A major goal is to prevent permissions (specifically high-risk) from proliferating across various cloud management tools.

The TAG Cyber team recently sat down with Raj Mallempati, Chief Operating Officer of CloudKnox, a cyber security company specializing in cloud permissions management. We wanted to learn more about how insider threat, mismanagement of permissions, and suboptimal security hygiene could lead to serious vulnerabilities in cloud use.

TAG Cyber: Raj, what do you see as the central security challenge for companies that wish to move their infrastructure to the cloud?

CLOUDKNOX: In the cloud, an enterprise's security is only as good as its ability to control the access that their human and non-human identities have to their infrastructure. Because the actions that these identities can take are dictated by the types of permissions granted them, proper assignment, management, and monitoring are critical.

Cloud makes it quite easy to spin up new resources, and this rapid seamlessness is the main driver for migrating to the environment. The unfortunate byproduct of that lightning pace is this, however: wide-ranging permissions in the cloud are the norm and the result of high automation. And with over 40,000 (and growing) permissions across the key cloud platforms, it's nearly impossible to keep track of who has what, what is being used, and on which resources.

In most enterprises, there is an unfortunate and dangerous delta between permissions granted and permissions that are actually used. We call that the Cloud Permissions Gap, and it's growing ever bigger by the day in nearly every cloud environment. This gap is a fast-emerging cloud attack surface and proving to be fertile ground for both accidental and malicious permissions misuse and exploitation.

Enterprises often know how vulnerable they are but don't have the skill set or tools to adequately address the exposure. Over time, the problem becomes increasingly acute as organizations expand their cloud footprints without establishing protocols and capabilities to properly assign,

manage, and monitor human and non-human identity permissions across their cloud environments.

TAG Cyber: The concept of continuous security has taken on great significance in the community. Do you see continuous detection, remediation, and monitoring as critical requirements for cloud security?

CLOUDKNOX: Yes, I do. If identity is the new perimeter and the new entry point for attackers, then high-risk permissions will quickly become one of the most menacing threat vectors to cloud infrastructure for years to come. Mitigating that risk/threat is not a one-time project, but a continuous process, because the complexity of managing these dynamic environments will increase exponentially over time, considering that the various permutations of identities, permissions types, and resources across multiple cloud platforms will run into the millions and will be consistently changing.

TAG Cyber: If, as you referred to above, identity is the new perimeter, do you see identity and access management (IAM) playing a particularly important role in protecting cloud-hosted resources?

CLOUDKNOX: I think it is safe to say that identity has become the new digital perimeter and there is no turning back. I also see IAM as playing a key role in protecting cloud-hosted resources. The problem is that as more enterprises evolve their cloud strategies, they will be faced with legacy identity and access tools that were never meant to exist outside the enterprise. They are realizing that secure access and authorization to hybrid cloud and multi-cloud environments is a significant impediment to execution.

For example, many companies that are trying to employ the principle of least privilege (POLP) in their hybrid cloud are leveraging solutions that still use role-based access controls (RBAC)—a 30-year-old mechanism that was created in the pre-cloud era. The problem with this practice is that traditional RBAC only works in a static environment. This means that a typical privileged identity today has authority to perform many high-risk actions on a wide swath of critical infrastructure despite the fact that they only use and need a fraction of those permissions to perform their day-to-day jobs. This practice creates a significant, completely avoidable risk and grossly violates the best practice of POLP which clearly states the following:

"The Principle of Least Privilege (POLP) is a fundamental guideline for secure computing that restricts privileged identities to only the permissions they need to perform their authorized tasks." Therefore, enterprises will need to evaluate tools that will enable them to implement the principle of least privilege at a granular

high-risk permissions will quickly become one of the most menacing threat vectors to cloud infrastructure for years to come.

level across their hybrid cloud environments and prevent—or at least significantly minimize—the risks associated with incorrectly or overprovisioned human and non-human identities.

TAG Cyber: Are most of your customers now using multiple cloud services— and what are the challenges that emerge when you see this situation arise?

CLOUDKNOX: Yes, most of our customers are using at least one public cloud and are in the process of adopting additional clouds. The automation associated with cloud infrastructure has given enterprises the ability to scale to new heights in efficiency but has also introduced a new set of cloud-related cyber threats.

Just as the infrastructure has evolved, so have the attackers. They are quickly learning to take advantage of this automation to get their hands on the "keys to the kingdom"—a trend indicating an attack strategy targeted at the cloud infrastructure itself as opposed to specific identities or data sets.

TAG Cyber: I've heard you mention something called "privilege creep" across cloud services. What do you mean by this?

CLOUDKNOX: The Privilege Creep Index is a single metric that measures your ability to implement the

PoLP across your hybrid and multi-cloud environment. PCI is updated on an hourly basis and is a function of 1) the number of unused high-risk permissions and 2) the total number of resources an identity can access. We provide the PCI score at both the account level (e.g., AWS) and the individual identity level, giving security teams an immediate understanding of the cloud permissions gap across their cloud environment.

TAG Cyber: Any final security or compliance-related advice for enterprise teams who might wish to reduce their risk of transitioning to cloud services?

CLOUDKNOX: We like to recommend that every company operate under the assumption that the #1 risk to their hybrid and multi- cloud infrastructure is a trusted privileged identity with excessive privileges and the only way to manage that risk is to implement the principle of least privilege. If not, they run the risk of compromising every security system, policy, and procedure they've worked to put in place.

We believe that in the era of cloud computing, enterprises need to recognize that the complexity of managing identities and identity privileges will increase exponentially over time. They should consider that the various arrangements of identities (human and non-human)—in addition to permission types and resources—across multiple cloud platforms will run into the millions and make it virtually impossible to administer manually.

For enterprises to get ahead of this, there are a couple of recommendations we typically like to share, as follows:

1. Get a true understanding of your enterprise's risk posture by gaining the right level of insight and visibility into the surrounding environment, including:
   - Which identities (both human and non-human) can touch my infrastructure?
   - What permissions do they have?
   - What actions can they perform with those permissions?
   - How many are high-risk?
   - What permissions are they actually using? Not using?
   - Which resources are they performing actions on?
2. Based on these findings, enterprises should implement a risk mitigation plan by identifying identity permission right-sizing opportunities and enforcing it.
3. Continuously monitor and assess the activity and behavior of both human and non-human identities across your infrastructure to assess your risk profile on a regular basis.
4. Have the ability to quickly produce a forensic tail of all pr ivileged identity activity and resources impacted. This will empower your security organizations to quickly detect and remediate incidents and help you put preventive measures in place.
5. Manage the identity privilege lifecycle from a position of trust. It should never be about restricting permissions and inhibiting productivity but about giving identities the authority to use the permissions they need—when they need it—to do their day-to-day jobs.

AN INTERVIEW WITH JOE PAYNE, CEO, CODE42

DO YOU KNOW YOUR 3 KEY INDICATORS OF INSIDER RISK?

Data loss protection or prevention (DLP) is a 20-year old technology that was designed to protect organizations' "crown jewels"—i.e., their data. The original concepts for DLP were solid, yet actual implementations were painful, taking months, if not years, and created a tremendous amount of manual work. As a result, DLP failed to deliver adequate security. Nonetheless, companies still needed effective methods to protect data.

Over the years, as digital transformation impacted business operations, and as employees increasingly required 24X7 access to files, folders, and applications—without having to jump through hoops—security leaders knew that better data protection was required. Access to data is imperative, but overly permissive or unauthorized access introduces unnecessary insider risk.

Code42 takes a new and refreshing approach to data loss protection, looking at it through the lens of insider risk. We sat down with Joe Payne, CEO of Code42, to discuss the convergence of insider risk, workforce collaboration, and data security.

TAG Cyber: How have collaboration and remote work affected the approach to data security?

CODE42: Corporate culture change is happening en masse. Organizations strive to be faster paced, flexible, and fluid—it's all about speed. The business and IT leaders driving the digital culture realize creativity, ideas, and innovation can come from anyone, at any time, from anywhere. So, naturally, they turn to technologies like Slack, Zoom, Office365, and Google Suite to empower employees to be more collaborative, productive, and virtual. The highly collaborative, productive, and virtual technology provided—the culture created— has made corporate data more invisible, portable, transferable. The next great ideas within an organization are no longer classified and locked down on an owned and operated device or data center. They live in the cloud— unstructured, unlocked, and unleashed. Case in point: *

- 37% of employees use what they want on a daily basis to get work done
- 73% of employees report they have access to data they didn't create
- 69% of employees can view data they didn't contribute to
- 59% of employees can see data from other departments

More than a decade ago, data security approaches like DLP had very clear objectives: protect sensitive, regulated data by locking down access to that data, thereby reducing the risk of loss, leak, or theft at the hands of external or internal actors. While that sounds like nirvana, that approach is no longer effective. Digital business strategies have given rise to the collaboration culture. Work

increasingly happens via cloud- and web-based apps—driven by unprecedented and rapidly increasing levels of user, device, and data portability. Collaborative organizations are simply too fluid, too distributed, too complex, and too porous.

In the face of the collaboration culture, we need a mindset change in data security. It is not possible to identify or classify every sensitive file effectively across a complex, ever-changing organization. It is also not possible to define policies for all possible employee actions that may be harmful and then prevent those events from happening. The new data security mindset requires us to treat ALL data as sensitive. Whether it is source code, sales pipelines, HR data, marketing targets, customer lists, or financial information—it is all important. The new mindset requires us to watch all data activity, all the time; to allow first, then verify. Collaboration and sharing are absolutely good for workforce productivity, so we allow it. But we always verify the sharing is not a risk to data. Instead of stopping risks by categorically blocking abnormal activity, security teams must prioritize threat detection and response. They must embrace a "trust but verify" approach to find the right balance between workforce collaboration and risk mitigation. But looking at sharing after it occurs (instead of blocking the sharing) we can allow for productive collaboration while protecting against misuse.

TAG Cyber: How is Code42 Incydr, your data risk detection and response platform, different technologically from traditional data security like DLP?

CODE42: Having to define in real time the what, who, where, and when of insider risk is complicated, error prone and slow. DLP products intended to secure data actually force you to do all the work. They take lots of care and feeding. They turn security teams into Big Brother. Collaboration is crippled. Policy exceptions grow. Blindspots increase and data still leaves. Quite frankly, it's a broken and painful approach. Code42 Incydr takes a different approach focused on speeding detection and response.

Code42 Incydr detects risk by observing all file movement, creation, deletion, and modification activity that takes place across computers, cloud, and email—whether those actions are approved by security or not. It sees activity like web uploads, syncing files to personal cloud accounts, printing files, or transferring them to a USB. Direct integrations with corporate cloud services detect public or untrusted file sharing while integrations with email services detect when file attachments are sent to untrusted recipients. It gives security teams their first real understanding of employee file activity across their entire environment.

The beauty of Incydr is its signal. Although it sees everything, it only visualizes and alerts you to the events that indicate insider risk.

Security teams are swimming upstream trying to force fit old technology for the new way we work.

Incydr filters out the noise of trusted activity to reveal only the risks that require security's attention. It enriches detected activities with much needed context on the vector, file, and user. This includes the type of files involved, whether the activity took place remotely, was performed during hours when the user is not typically active on their device, and even provides the ability to review full file contents. It does this at a company-wide level and on a per-user basis.

Incydr provides the facts security teams need to take an informed and right-sized response to insider threats. And, unlike traditional security tools, you can get it up and running in a matter of days. This is because Incydr doesn't require data classification or policies to be created. If you track activity of all data for all users, you don't spend months defining specific policies and tagging all your data. It's a game changer when it comes to securing the collaboration culture.

TAG Cyber: How does the current economic crisis and an increasingly remote workforce change how businesses look at protecting their data?

CODE42: Pre-COVID-19, 29% of employees worked from home. Post-COVID-19, more than 80% of global organizations have encouraged or required employees to work from home. Therein lies a problem. To safeguard data, generations of security professionals have learned to diligently identify and classify it, and then block users from accessing and sharing via policies. This old approach to data security was never designed to protect data outside the perimeter of the corporate network. Security teams are swimming upstream trying to force fit old technology for the new way we work. Here's what we found in the 2019 Code42 Data Exposure Report about insider risk:

- 69% of organizations breached due to an insider had a prevention solution in place at the time
- 78% of information security leaders believe that prevention strategies and solutions are not enough to stop insider threats
- 77% of security professionals say prevention solutions like DLP are difficult to implement

In a world where every employee is suddenly working from home, the very policies and processes organizations have put into place to secure data have been rendered obsolete. It demands we, as a security industry, rethink, reimagine, and rebuild what data protection means where working remotely is not an employee perk, but the norm. We're living in a time when emailing, Slacking, and sharing Google docs—whether from our kitchen, cubicle, or coffee shop—are the norm.

The challenge is, the cloud-based collaboration tools that companies have rolled out to move faster and be more productive are the same vectors used for exfiltration. Data

security must be built for modern times. Regardless of where your data moves—across computers, clouds, email, and web browsers— when it comes to data protection, businesses need to be able to distinguish between everyday collaboration and the events that put data at risk. The end result is a workforce that remains productive and a business that remains secure.

TAG Cyber: What are some of the concerning trends about employee data use and access, and what can CISOs do to better protect the organization?

CODE42: Too many times, we see companies pour 90% of their investments into preventing external threats and leaving the last 10% of their budgets to control internal threats. The reality is that's just not enough protection and there's not enough visibility — especially in our world today where millions of employees are working off the corporate network, sharing sensitive company files across Slack and then moving them to a personal Dropbox account for "safe" keeping.

Some reports say two-thirds of breaches are inside jobs. Others might argue the percentage is lower. And we could see why unsuspecting organizations— that are just plain unaware that their data is being exfiltrated— might think that insider threats are lower risk. Our advice is: Don't be naive. Over 60% of employees admit that they took data when they left their last job. CISOs must reassess the insider risk that exists inside their organizations.

To help CISOs, we put together a series of questions that cover three key areas of insider risk: remote employees, departing employees, and high-risk employees.

Remote workers. We are living through the largest shift in work culture in our lifetime. The spread of the corona virus has forced many people to work from home. A decision that, while necessary, has put a strain on security teams. Suddenly, they are on the hook to manage data risk beyond the perimeter and do it at scale. Doing so requires some real gut-check questions:

- Do you have visibility into all employees' off-network file activity?
- Do you know what trusted and untrusted collaboration tools employees are using?
- Do you know what data employees are moving, when they move it and where?

Employee departures. Insider risk is not an isolated incident—it's an everyday occurrence. Think about this: We are experiencing some of the highest unemployment rates our country has ever seen, with millions of job losses over the last few months. How many of those employees walked out the door with your customer lists, source code, or sales pipeline data? Do you know?

- When someone leaves your company, what do you do to ensure they aren't taking confidential information with them?
- If an employee who is leaving returned a wiped laptop, could you determine what confidential information that employee accessed before wiping the laptop?
- If you suspect that a key employee took confidential information to a competitor, how would you investigate? How long would that take? What would it cost? Would you have enough information to pursue litigation if required?

High-risk employees. To ensure business continuity during a crisis, it is important to have a clear picture of employees who are considered high risk. Workers could be considered high risk because of the data they produce or have access to, and/or because of their data controls and privileges.

- If one of your key employees had their corporate IT credentials compromised, could you detect if the account was being used to transmit confidential information outside of the company?
- Which employees have access to your most sensitive information, including customer lists, source code, product roadmaps, and more? What technology are you using to detect if they misuse that information (either intentionally or accidentally)? How would you know if an employee took sensitive data? When would you know?
- What steps would you take to prevent misuse of your trade secrets by employees?
- If one of your employees accidentally shared a file outside of your organization, how would you investigate to determine whether you had any reporting obligations to regulators or customers?
- Have you educated your employees, especially privileged employees, about how to detect and avoid falling for potential phishing or malware campaigns?

Of course, this is not an exhaustive list of questions for every possible insider risk scenario, but they are a baseline for assessing your level of visibility or lack thereof. As a security industry, we are navigating some uncharted territory. New data security challenges have been thrusted upon us, and they're rooted in cloud, collaboration, and speed. If we are to survive in the short-term and thrive long-term, we must rethink, reimagine and rebuild how we do data security.

**From the Code42 Data Exposure Report 2020*

AN INTERVIEW WITH AARON HIGBEE, CO-FOUNDER AND CTO, COFENSE

SECURITY AWARENESS HAS MOVED BEYOND BOX CHECKING

Information security books from the mid-2000s are nerd comedy. Three tiers of firewalls? Attackers didn't read those architecture books. Instead, they sent emails to people. People are now our first and last line of defense in cyber security. The reasons are myriad, but most of all rely on the fact that people need access to resources—data, files, systems—to do their jobs. And how does that access happen? Via legitimate authorization. If a cyber criminal can obtain the means by which a legitimate user accesses resources, conducting a full compromise becomes much simpler.

For many years, phishing has overwhelming been the main tactic used by threat actors to initiate cyber attacks. But it's also been proven that empowering employees to report suspicious email asymmetrically disadvantages the attacker. Attackers can create a phishing tactic that defeats a technical control 100% of the time. But attackers cannot fool 100% of humans 100% of the time. Cofense specializes in preparing humans to be an active part of detection and response. We spoke with Aaron Higbee, Co-founder & CTO at Cofense, about how organizations can win in phishing defense.

TAG Cyber: Security training programs have been around for years. Why isn't awareness enough?

COFENSE: At the heart of this, there are three problems with awareness programs as standalone activites:

1. Awareness coupled to compliance training frames the activity poorly. My dog loves peanut butter. How does she know when her medication is in it? A seasoned employee can sniff compliance training in the air no matter how clever you package it.

2. "Awareness" assumes the goal is to make people aware. In 2020, are people unaware of phishing? If you make them aware, do you win?

3. If you are going to borrow productivity from humans to invest in awareness, the time should be proportionally tied to the threat. Example: Email phishing vs. USB thumb drive attacks. How much security operations time do you spend each year on attackers dropping USB sticks in the employee parking lot?

Security awareness has moved beyond checking a box to deliver annual training. As organizations continue suffer from cyber security incidents, there has been a shift to focus on "changing behavior" when it comes to protecting the organization.

TAG Cyber: What are some of the new tactics and techniques you've observed cyber criminals using against enterprises?

COFENSE: Attackers are using cloud platforms to defeat the defensive strategies of secure email

gateways (SEGs). The phishing attacks of yesterday used tactics like email spoofing, look-a-like domains, or hosting phishing kits on compromised WordPress blogs. Today, they can deliver the entirety of the phishing attack on Office365, making it nearly impossible to filter.

The majority of attacks today are credential phishing. Once a threat actor has access to credentials, they can now move about the organization's single-sign-on solutions as a legitimate user. As a result, organizations are trying their best to adopt multi-factor-authentication. Great! But this won't solve phishing. We are in the early stages of watching phishing evolve into tricking users into granting authorization to attacker applications designed to pillage data.

Attachment phishing, while on the decline, is evolving too. Maybe it's a link (behind a URL redirect designed to fool a SEG) to a website that prompts the user to download a file. Or an old filetype that was packaged in a clever new way.

TAG Cyber: Most enterprises have a SEG deployed. What is Cofense Vision and how does it complement the SEG?

COFENSE: Fact: Some of your humans will tell you about a phishing attack in progress within seconds of receiving it. This isn't an inflated opinion. Ask anyone who has ever conducted phishing simulations. Unfortunately, the catch phrase "the human is the weakest link" has stymied security operations teams worldwide. SEGs have been in the hands of "the mail team" or the "open a ticket for IT" workflow.

Enterprise mail and the security operations teams have different business objectives—one to keep email flowing, while the SOC defends the perimeter to protect the organization. The mail team doesn't want security running performance impacting queries. Legal, HR, and compliance teams, understandably, can't sign-off on giving full email access to security with no accountability. Cofense Vision solves this.

The return on investment for phishing simulations isn't awareness; it's stopping active real phishing attacks.

The return on investment for phishing simulations isn't awareness; it's stopping active real phishing attacks. Minutes and seconds matter. One hundred percent of the phish seen by the Cofense Phishing Defense Center have been found in environments protected by SEGs. We built Cofense Vision to allow the SecOps team to act quickly to remediate phishing reports that bypassed the SEG. Is this a legit Excel attachment with a macro? Or is it malware? Our solution set helps balance the inherently porous nature of the SEG. Cofense Vision buys time for SecOps by allowing them to quarantine the email enterprise wide while they do their analysis. If the attachment was legit, Vision will put it right back in the user's inbox seamlessly. Vision can also be used

as a purpose-built email hunting platform for other IOCs, while satisfying compliance with an audit trail. It has a UI, it integrates with Cofense Triage beautifully, but you don't need those to use it. The API can do everything— making it flexible to work with in-house or with commercial automation tools.

TAG Cyber: What is the value of human analysis in the phishing protection process?

COFENSE: Technology is evolving at such a parabolic curve that it's hard to fathom what the future brings. That said, our best computer scientists haven't created an algorithm that mimics human intuition. Using your human brain, check out a few examples of what humans have caught that algorithms missed: https://cofense.com/real-phishing-threats/

Well-designed continuous phishing simulations level-up intuition, leading to higher report quality to SecOps.

Phishing tactics, since inception, evolve to evade automated detection. Investments in automation saves time for your experts by reducing time-sucking clutter. Human-assisted analysis, whether we like or not, is the only safety net that exists.

TAG Cyber: What kind of risk reduction can organizations expect when they deploy technology like Cofense Vision?

COFENSE: Customers that have deployed Cofense Vision have reported that they've been able to remediate a phishing attack within minutes.* This is significant considering that 65% of organizations take more than 5 minutes to detect a typical phishing email after it enters their networks, 30% take from 6 to 30 minutes to identify a phishing attempt, while another 14% take from 31 to 60 minutes for a detection. The Cofense intervention transforms phishing into a nuisance infection instead of it metastasizing into a catastrophic data breach.

There are two major metrics in incident response: mean time to detection (MTTD) and mean time to remediate (MTTR). By reducing the incident response timeline, the organization can greatly reduce their risk when it comes to phishing threats, strengthen their security posture by neutralizing threats evading other security tooling, and significantly lower risk.

** https://www.informationsecuritybuzz.com/articles/cybersecurity-labor-gaps-and-manual-phishing-detection-efforts-aid-email-vulnerabilities/#:~:text=Nearly%20one%2Dthird%20(30%20percent,60%20minutes%20for%20a%20detection.*

AN INTERVIEW WITH WITH KISHOR VASWANI, CHIEF STRATEGY OFFICER, CONTROLCASE

SUPPORTING COMPLIANCE AS A SERVICE

IT Security and compliance are greatly complicated by the myriad different frameworks and certifications that are required for the typical enterprise. These include PCI-DSS, HIPAA, ISO, and many more. For most organizations, the only reasonable solution has been to automate the process, and IT governance, compliance, and risk (GRC) tools have thus emerged as one of the most important aspects of modern enterprise security.

We recently spent time conversing with Kishor Vaswani from Fairfax-based ControlCase to develop insights into how they are streamlining this automation with compliance solutions that are delivered in an as-a-service manner. The results appear to be successful, and we were keen to understand whether this approach might help more enterprise teams deal with their compliance burden. Here is a brief digest of our conversation:

TAG Cyber: Tell us first about the company. When were you founded and what's been your value proposition for enterprise customers?

CONTROLCASE: ControlCase was Founded in 2004. We excel at two things:

1. We help companies achieve their IT security certifications with ease and without breaking the bank. We certify to regulations including PCI DSS, SOC, ISO 27001, HIPAA, GDPR, etc.

2. We provide a technology-driven continuous compliance solution that provides peace of mind that environments are secure and risk is reduced.

TAG Cyber: What has been your experience in assisting customers with their compliance? Has it been the process? Attestation? Understanding the requirements? Perhaps all of the above?

CONTROLCASE: Great question! What really sets us apart is that we are not a checkbox auditor; we adopt a partnership approach in all our engagements. So, because of that, we start at the beginning—really understanding our customer's environment and exactly what is driving them in their compliance process. We become an extension of their IT security compliance team to understand their motivations for, business processes used, and any gaps between current state and achieving compliance. Then we support them through remediation before moving to a final audit. To answer your question directly, it's really all the above; we have a tried and tested methodology that takes away audit fatigue for our customers and gets us to our goal in harmony.

To be honest, many of our clients battle with the issue of which regulation they need to be compliant with.

TAG Cyber: Do you see the possibility of some compliance framework consolidation in the coming years? It sure seems like there might be too many different security compliance requirements standards.

CONTROLCASE: Yes absolutely; our research has found that most of these IT security regulations can be easily mapped to each other. To be honest, many of our clients battle with the issue of which regulation they need to be compliant with—because you're right, there are so many.

As a result, we support clients who require compliance with multiple regulations so the mapping we have done eliminates repetition and saves both time and money. We certainly see consolidated frameworks coming in the future.

TAG Cyber: How are customers responding to your One Audit approach? Do they have to modify their internal compliance programs to use your service, or has the integration been simpler?

CONTROLCASE: Another great question! Companies that care about security have been very responsive to our One Audit solution. In a nutshell, it allows us to collect evidence once and certify companies to multiple regulations. Because we partner with our clients and understand the business requirements that are driving the need for multiple certifications, we have really focused on using smart technology to enable automation. This has created a seamless solution that integrates with clients' environments so that we can collect evidence more efficiently, manage security and continuous compliance, as well as keep costs and stress to a minimum.

TAG Cyber: What do you see on the horizon for compliance programs? Do you see integration of security and privacy certifications, for example?

CONTROLCASE: I believe compliance programs are going to become more stringent—the easier it is and the more we share data, the more stringent these regulations will become. And I believe it is a necessary transformation that has already started to happen. Most regulations cover aspects of both security and privacy—it's just that there is usually a choice on the privacy aspect. In answer to your question, I truly believe we will eventually come to a place where compliance programs find the perfect harmony between security and privacy

AN INTERVIEW WITH WITH EDUARDO CERVANTES, CEO, CORSA SECURITY

NETWORK SECURITY VIRTUALIZATION FOR ENTERPRISE AND LARGE NETWORKS

Protecting networks from the internet and internally between trusted zones has long implied the deployment of DMZ-oriented firewalls, and this remains an important functional requirement. The problem is that with ever increasing traffic volumes, changing traffic mixes, and more and more network traffic encrypted, these firewalls have to be replaced often to give the network complete traffic inspection and better threat protection.

An interesting and effective alternative to frequent firewall replacement involves using virtual firewalls to scale traffic inspection and threat protection just like we saw in the data center's early days. But this virtualization must be turnkey, which means tight integration of the orchestration, management, and operation of the virtual firewalls that are so essential when connecting an enterprise or other network to the internet and between zones. The result is complete visibility, even with SSL/TLS traffic, and the ability to turn on all NGFW features without impacting performance, leveraging existing firewall policies, and deploying without changing the architecture.

We recently spent time with Eduardo Cervantes, CEO of Ottawa-based Corsa Security, to discuss their creative approach to offering turnkey network security virtualization driven by simple and intelligent orchestration. The Corsa Security platform uses virtual next-generation firewall capabilities for complete traffic inspection, including SSL/TLS visibility, and makes this process flexible, extensible and secure.

TAG Cyber: What do you mean when you reference network security virtualization? Does this replace the firewall?

CORSA: Virtualization is not a new concept for many elements within the network or data center. However, the network firewall has been one area that has lagged behind the others when it comes to virtualization. Simply put, the Corsa Security platform leverages virtualization to scale network security, but we make it turnkey so it can be easily deployed and scale as needed. When you deploy our platform, we are not asking you to replace your firewall, as it performs some critical functions and it can be quite disruptive to remove. But instead of upgrading to a larger hardware platform if you need more performance, what we are offering with our solution is a way to quickly add more firewall capacity at a lower TCO. We give you the flexibility to adopt a pay-as-you-grow model so you are only paying for the inspection capacity that you need and when you need more you can simply order what you need with the click of a button.

TAG Cyber: How important is SSL/TLS visibility and do you see enterprise teams handling this function efficiently?

CORSA: SSL/TLS visibility is absolutely critical to enterprises. More than 75% of traffic is now encrypted—which is a good thing for security and privacy. However, cyber criminals also see the benefit of encrypting their attacks too. If the firewall can't keep up to give visibility into these ever-increasing

encrypted traffic volumes, then enterprise security teams are forced to tune back firewall rules and simply let traffic through.

An option that is both effective and brings efficiencies, that is especially relevant for enterprises going through digital transformation, is to virtualize firewalls at the network gateway and between zones. Virtualization fits within tight budgets while delivering improved performance and flexibility so networks inspect all traffic and close holes in their defense.

TAG Cyber: I've heard you reference software defined firewall in the context of your solutions. What do you mean by that?

CORSA: We talk about software-defined firewalls as a way to differentiate what we are offering from traditional hardware-based firewalls. It helps to set a context for our audience in terms that they already understand such as software-defined networking and SD-WAN, for example.

What we mean is that when you need to boost the performance of your firewall, you don't need to buy a purpose-built physical device. Instead, you can leverage commodity servers, virtualization, and software-defined principles to scale your traffic inspection and threat protection all wrapped up in a turnkey platform so you don't need DevOps.

Another reference we often make when explaining our solution is to draw a parallel to hyperconverged infrastructure, which is widely leveraged for storage, and say we are offering a similar HCI package for security.

If the firewall can't keep up to give visibility into these ever-increasing encrypted traffic volumes, then enterprise security teams are forced to tune back firewall rules and simply let traffic through.

TAG Cyber: Your marketing briefs reference firewalls potentially "burning with too much traffic." This is an interesting image—and I was hoping you might expand on what you mean by this designation.

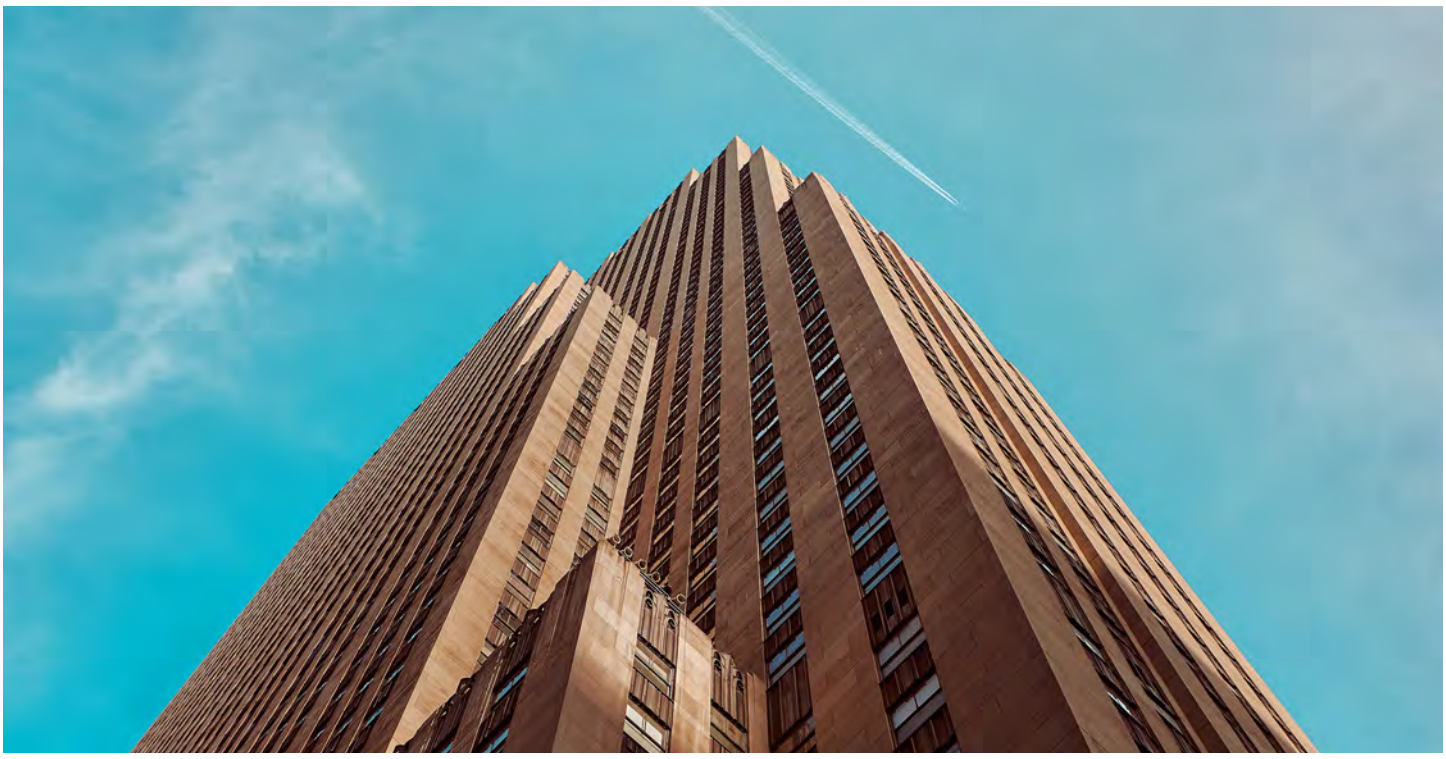
CORSA: It's definitely an image that we have seen resonate with our audience and grabs attention. For us, it clearly captures the issue that these single-purpose hardware devices face. They are metaphorically on fire because we are simply asking them to do too much. No single CPU complex can be expected to do all that a firewall does while traffic volumes continue to increase with the vast majority of it encrypted.

The only way, in our opinion, to douse the flames on your burning firewall is to leverage virtualization and multiple CPUs to not only give you complete SSL/TLS visibility but also the opportunity to turn on all your firewall features without fanning the flames. Just like the firefighters you see in some of our marketing material, we have the expertise needed to make this network virtualization turnkey and automated so you don't need to do the heavy lifting and put out the fire yourself.

TAG Cyber: What are some trends you see in this space in the coming years? Do you see zero trust, for example, continuing to grow in importance?

CORSA: At the start of this year, we likely would have talked about 5G, IoT, and maybe even cloud as the key trends impacting security. However, COVID has clearly changed all of our priorities, and the trends we are talking about now involve remote working and the need to adapt to changing conditions quickly.

So it's a lot about automation and virtualization. I believe that these changes which have impacted organizations everywhere will continue to affect the security industry for the foreseeable future. That's why the ability to leverage virtualization to scale key functions and then do so in an automated fashion is absolutely critical. We have seen a huge increase in our platform this year because we make both of these things possible. As for zero trust, that's been with us for a few years now since mobile and IoT devices began to proliferate and yes, it continues to grow in importance. With more and more people working from outside the office, it will become even more relevant because employees are connecting to critical data and resources from largely unprotected home or public networks. It's crucial that security teams make zero trust their philosophy and continue to invest in zero trust architectures they implement across all areas of their networks, not just at the device edge.



AN INTERVIEW WITH WITH PAULO SHAKARIAN, CEO, CYR3CON

DRIVE INTELLIGENT DECISIONS FOR VULNERABILITY MANAGEMENT

Cyber threat intelligence is regarded as the fuel for proactively identifying threats before they become exploits. Over the last ten years, companies have significantly ramped up their threat intelligence collection, bolstered by commercial products and highly skilled cyber threat analysts, many of whom hail from the military threat community. However, for cyber threat intelligence to be actionable, it needs to be predictive and specific enough for security operators to act upon.

"Actionable" has been the sticky wicket of threat intelligence for a long time, not because commercial or open source products are bad, but because there is so much data and information being fed into them and often not enough analysts reviewing the data to react to it in a timely fashion. For these reasons, the founders of CYR3CON decided to take a different approach to exploit prediction. TAG Cyber spoke with Paulo Shakarian, CEO of CYR3CON, about threat identification and actionability.

TAG Cyber: Let's start with a quick overview of the CRY3CON platform and how it differs from traditional threat intelligence or vulnerability management technology.

CYR3CON: CYR3CON is designed to drive decisions around vulnerability management—and the ability to do so through machine learning sets us apart. Our customers—including some of the best teams in security—use CYR3CON to identify threats to vulnerabilities they do not get from anywhere else. Our technology accomplishes this by automatically combining and analyzing multi-sourced intelligence gathered from places like social media, the dark web, deep web, and even security research sites to predict what vulnerabilities will be used by hackers. The results are provided through a web-based user interface as well as a REST based API.

TAG Cyber: Why do companies fail in threat intelligence efforts when using CVSS alone?

CYR3CON: CVSS was never designed to be predictive—it is totally devoid of any type of threat intelligence. Take for example CVE-2018-13379*—a "medium" severity vulnerability per CVSS v2. Just last week, it was reported that Russian hackers (CozyBear) were using it steal COVID-19 vaccine research**. Meanwhile, there's about a year's worth of threat intelligence which tells a much different story. This example is just one of many—multiple scientific peer reviewed papers have shown that CVSS is not predictive.

TAG Cyber: CRY3CON uses its own rating system, the CyRating. What are the elements that comprise a CyRating and how is it different than a CVSS?

CYR3CON: The CyRating of a vulnerability tells you how many times more likely a vulnerability

This example is just one of many—multiple scientific peer reviewed papers have shown that CVSS is not predictive.

is to be exploited than average. It is produced by a machine learning model that considers threat intelligence data gathered from various hacker communities (social media, dark web, etc.) and other sources, including past exploits. The machine learning model essentially identifies patterns in the threat intelligence that lead to exploitation of a vulnerability. This is totally different than CVSS, which is not intelligence-driven.

TAG Cyber: Your company resources mention the "ignored threat." What do you mean by that, exactly, and what can companies do when, for instance, they can't patch a known critical vulnerability?

CYR3CON: If you consider the Equifax breach of 2017, that team knew about the vulnerability but decided not to patch or mitigate. They clearly did not consider the threat to that vulnerability to be significant. Every company makes decisions like this about vulnerabilities. In the Equifax case, they ended up ignoring the threat.

CYR3CON identifies which vulnerabilities have an associated, elevated threat. Our clients not only use this to execute routine mitigation actions such as patching, but also justify IT projects to upgrade or replace systems, design other controls or mitigations, or isolate the systems in question.

**an Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests*

***Per CVSS Version 3.x, CVE-2018-13379 was upgraded to "critical."*

AN INTERVIEW WITH WITH SAM CURRY, CSO, CYBEREASON

ADVANCED ENDPOINT PROTECTION, DETECTION, AND RESPONSE

Endpoint security has emerged as a salient aspect of cyber protection programs. In particular, support for the full range of protection, detection, and response activities across the attack lifecycle has become imperative, especially with cyber threats from nation-state actors becoming so difficult to contain. Enterprise teams have thus had to accept that some threats are likely to require response, regardless of any preventive actions that might have been taken.

We recently had the opportunity to sit down with Sam Curry, Chief Security Officer for Boston-based Cybereason. Sam has been an expert practitioner and visionary in the security industry for many years, and he provided a fascinating glimpse for us into the best practices that exist in this new endpoint protection, detection, and response method.

TAG Cyber: Sam, it seems like the focus has shifted from prevention toward detection and response in the endpoint security solution space. Is this an accurate view?

CYBEREASON: Absolutely—prevention works best with first order chaos systems, like natural systems and where there isn't intelligence behind adaptation. For instance, COVID-19 is a threat in the first order chaos system of biology and a hurricane is a threat in the first order chaos system of meteorology. However, like market competition and legal conflict, or perhaps military or law enforcement systems, security is a second order chaos system. That means that any preventative measure you put in place is going to have a shelf-life before it gets bypassed. And that is incredibly frustrating when you first encounter it, but there is a way to turn the tables: you have to get very good at applying intelligence in defense. That means the name of the game is about detection and response and the efficiency of the machine you establish to do this. Call it EDR, call it XDR, call it SOAPA, or anything of the sort—it's about the machines we establish in defense to get more and more efficient at finding, stopping, and improving over time to deter the intelligent opponent.

That's the game, now and forever, really, or at least until we commoditize AI to such a degree that it becomes moot; and that's not happening any time soon regardless of vendor hype.

TAG Cyber: What are the key requirements you're hearing from enterprise customers regarding their needs in the endpoint security area?

CYBEREASON: There are a few directions here. First, "do no harm" is a biggie. Stop tying up CPU, interfering with business and operations, and acting

Stop tying up CPU, interfering with business and operations, and acting like the special snowflake in IT.

like the special snowflake in IT. We're seeing this when it comes to privacy as well—if security vendors are not built with privacy-by-design,* the businesses that use them will struggle to adapt to a changing landscape of privacy-driven regulation and consideration. "Do no harm extends" farther than performance costs.

Second, ding the unfindable and make it actionable. Sooner, more completely, more reliably. Enable the human-based intelligence to be as efficient as possible. Play nicely in an ecosystem.

These are, frankly, the cardinal rules of security. We in security exist for a purpose, and that's to enable business and to improve over time at rooting out the disease in the system—malware, sure, but first and foremost, the real threat: adaptive men and women behind the advanced toolkits.

TAG Cyber: Do you see any trends in the attack space? Specifically, we're wondering if nation-state attacks have gotten more intense, and whether enterprise teams have much chance of actually stopping these exploits?

CYBEREASON: There are several trends among attackers. First, move to where there is more power and less defense. It's simple game theory, really. Fileless malware is the perfect example of this. Go to the company's blessed, ubiquitous, most powerful tools and abuse them. Use the tools of the defenders against them. For instance, the reflex to re-image ransomware-infected machines in IT means that attackers can drop ransomware like a grenade left behind in a room and let IT clean up the mess and helpfully delete forensic evidence.

Another great example is the use of unique signatures. The attackers monitor malware repositories and whether that instance of Poison Ivy is one-of-a-kind, and not only will the hash never help find another instance, it will provide a nice canary in the coal mine of a defender's network to let the attackers know the fight is on. Other techniques are obvious: proliferate tools that create noise, use the things that work, like DDoS and phishing, and get results.

It's always about the results, which means that in a conflict between intelligent opponents, it is a race in first and second derivative for innovation. In response, the move must be to look for better telemetry and something more effective than mere SIEM 3.0.

TAG Cyber: What do you think is coming in the next decade or so in the endpoint security space? Are you optimistic that risk will be reduced?

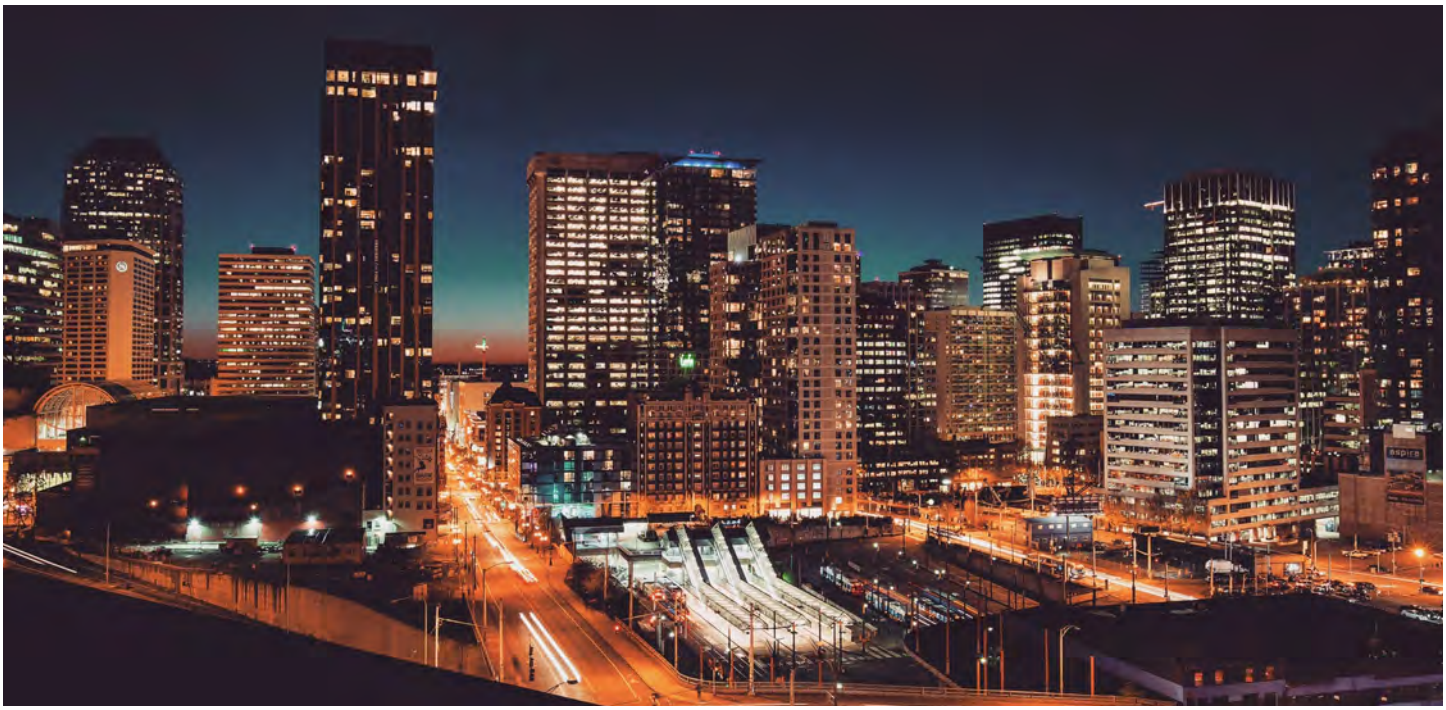
CYBEREASON: I am optimistic because we can and will adapt. The community of defenders and the potential to win is there. We need to do a lot, though. We have to get hardware roots of trust working for us, strong crypto done right, mosaics (rather

than chains) of trust, information sharing done better (hint: it's not about symmetry in sharing), privacy enforcement, least privilege, no default identities, proper federation, more effective cyber platforms (I'm looking at you, XDR, for this one!), and so on.

We also need to develop telemetry such as indicators of behavior (IOB) that have more permanence and get us higher in the "Pyramid of Pain" —those that are able to track attackers regardless of their innovation and how they dodge and weave. One way to do this is to put pressure on vendors that dedicate all their efforts to feeds and IOCs and have them, instead, build up the ecosystem and sophistication of the IOB.

The list is long, but even small advances will help enormously. We need to measure ourselves on our adaptability, to use automation intelligently, to achieve scale. We don't need AI to do this, although it helps. What we need is to make the defenders, the mark-1 carbon-based intelligence, the cyber warfighter, if you will, as effective as humanly possible—and ever improving.

** https://www.forbes.com/sites/samcurry/2020/07/20/privacy-by-design-responding-to-the-us-eu-privacy-shield-ruling/#330ea0a91940*



AN INTERVIEW WITH WITH RALPH P. SITA, JR.
PRESIDENT / CO-FOUNDER, CYBRARY

ONLINE CYBER SECURITY EDUCATION, BY PRACTITIONERS, FOR PRACTITIONERS

Cybersecurity is an ever-evolving field. New threats, new defense techniques, and new technologies continue to emerge. In addition, the demand for skilled and capable cyber security talent far exceeds the supply. Savvy practitioners know their worth is tied to how much knowledge and hands-on experience they can demonstrate to prospective employers.

As such, continuing education and skills building is imperative to not only landing a role, but also for building a fulfilling cyber security career. Over the years, online training has become a popular option for cyber security practitioners—who generally don't have an abundance of free time, given market dynamics. One of the leading platforms for cyber security- specific career development is Cybrary. We spoke with Leif Jackson, VP of Content and Community, to talk about the space, Cybrary's offerings, and how online learning is evolving given the health-related crisis of the past few months.

TAG Cyber: First, can you please explain how Cybrary's model differs from other learning platforms and the types of courses on offer?

CYBRARY: Absolutely. As Albert Einstein once said, "I do not teach anyone, I only provide the environment in which they can learn." For three million cyber security and IT professionals, Cybrary is that environment to learn. So why do our customers choose us? We have the fastest growing catalog of learning content in cyber security today. This is because of our fantastic creator network and the amazing breadth of vendors we offer on the platform. With most learning companies, you only have a single vendor, but with Cybrary, you have ten vendors across different specialties, verticals, and modalities.

The catalog itself has quadrupled in size over the past year. We have heard from our customers and students that our content velocity is what sets us apart from competitors, as they know we are moving and evolving with the industry. We have three main modalities of content: video courses, virtual labs, and practice tests. We lace all the content together so there is a teach, practice, assess model for the learner.

Some of our most popular courses relate to preparing for all aspects of critical certifications in the field, with certification bodies such as CompTIA, (ISC)², Microsoft, and AWS, among others.

In addition, and of tremendous importance, is our model, which is: by cyber security practitioners, for cyber security practitioners. Our instructors are all practitioners or former practitioners, so they are teaching from a "how to" level instead of at a theoretical level. When it comes to career development, learning from someone with

hands-on experience is invaluable.

TAG Cyber: Cybrary has been at this a long time. How is your approach to career development changing with remote workforce dynamics?

CYBRARY: Great question. We have certainly reprioritized our roadmap based on the current COVID-19 pandemic to focus on protecting companies against the multiplication of endpoints. We've seen from our customers that COVID-19 has accelerated trends on cloud migration and cloud security, as there is less access to on-prem data storage centers and a greater number of endpoints and devices touching corporate resources in the cloud. We have also been forced to change the way we work as an organization, which enables us to relate to the challenges our customers are currently facing.

TAG Cyber: You offer a mixture of hard and soft skills training. Both are important, but are you seeing more demand for any one area versus another?

CYBRARY: We are certainly seeing more demand for certifications- and cloud-based content. Most organizations now are operating in the cloud and have many team members they need to upskill to secure the cloud. That said, soft skills are important; we find that cyber security professionals often develop these soft skills later in their careers, when they're promoted after years of good technical work. Many of the best cyber security professionals grow up online and largely hone their technical skills before they start to build more team-oriented, management skills. But the ability to lead teams and communicate can't be underscored enough as security professionals grow personally and professionally.

TAG Cyber: What are the areas you see growing in importance for cybersecurity practitioners and leaders over the coming 12-18 months?

CYBRARY: I think clearly the cloud and everything about the cloud. The major cloud providers are changing so fast, there is simply no way you can keep up without making the commitment to constant learning. This has become critically important with more and more organizations shifting to a remote workforce as a result of COVID-19.

Set goals and stick to them. Give yourself time to learn. We suggest setting aside time each morning

TAG Cyber: How should prospective students approach training?

CYBRARY: They should always be learning. I recommend prospective students learn about and stay up to date on the latest trends in data science and security and, of course, cloud security. There are so many distractions, but you have to think about your brain like a muscle. It needs constant growth. Set goals and stick to them. Give yourself time to learn. We suggest setting aside time each morning to learn because that's generally before the daily distractions start setting in and you're forced to concentrate on many things at once.

AN INTERVIEW WITH WITH MIKE COTTON, VP OF RESEARCH & DEVELOPMENT, DIGITAL DEFENSE

ELIMINATING EXPLOITABILITY

Vulnerability management has been a staple of cyber security since the turn of the century. Enterprise security teams consider it a "must have" capability for understanding potential areas of concern within their networks. Yet, traditional vulnerability scanning is accompanied by numerous challenges: the abundance of known and reported vulnerabilities makes it difficult to keep track of and triage every potential issue; criticality/risk rating are sometimes not reflective of the potential threat to an individual organization; and organizations with hybrid environments may have to track vulnerabilities differently in each environment.

Yet, these challenges don't reduce the need for vulnerability and threat management. Without visibility into the internal and external attack surface—both of which are growing exponentially—the security team has little chance of patching vulnerabilities and remediating threats. We recently spoke with Mike Cotton, Vice President of Research & Development at Digital Defense, about vulnerability management and today's challenges.

TAG Cyber: Digital Defense has been around for almost two decades. How has vulnerability management shifted, especially recently in light of extensive work from home?

DIGITAL DEFENSE: As businesses adopt cloud-based and hybrid environments, vulnerability management has trended toward cloud-based models that can handle auditing multiple pockets of corporate technology on different networks and cloud-based infrastructures. Response to the rapid shift to work from home— and the expanded attack surface that came with it—accelerated this trend.

Additionally, because more of the global workforce is at home, there are more devices that are not always on the network. This is driving the need for vulnerability management solutions to use both agent-based and agentless scanning capabilities, rather than one or the other.

TAG Cyber: The Frontline.Cloud™ platform is cloud native. Why is that important?

DIGITAL DEFENSE: Since day one, we have prided ourselves on providing a platform that easily accommodates what businesses need as their environments evolve—traditional, cloud, and hybrid environments. Many businesses have evolved to offer their applications "as a service." It's something their clients are asking for and benefits their business with economies of scale and lower costs.

As a true cloud-native, multi-tentant, SaaS platform, Frontline.Cloud integrates deeply with cloud-platforms like AWS and Azure and is capable of fully utilizing the advantages that have driven so many businesses to migrate to the cloud. These include the abilities to scale up or down as needed, access vital technology from anywhere, incorporate data feeds from

many separate networks, and integrate seamlessly with next-generation cloud technologies.

Frontline.Cloud enables businesses to not only protect and remediate, but expand their offering by easily integrating with other third-party cloud-based security solutions. Traditional premises-based solutions can't do any of this efficiently.

TAG Cyber: Can an organization truly understand their risk and manage threats if they don't know the entirety of their attack surface? In other words, with IoT, work from home, and rapid application development, doesn't asset inventory become a critical part of managing threats?

DIGITAL DEFENSE: Yes, asset inventory is critical to understanding risk and managing threats. You must have a comprehensive understanding of your entire attack surface and what you need to protect. This is becoming more challenging in light of IoT, work-from-home, and cloud-services migration.

We advise our clients to start with asset discovery as a first step in building an efficient and effective vulnerability management program. Overwhelmingly, when we begin work with a client, we find there is an incomplete understanding of where their assets are and what services are running on them. We help them complete the view.

In work-from-home settings, endpoints may not always be on the network. Our solution is able to assess these endpoints with agent-based scanning technology. It's a wise complement to—not a replacement for—agent-less scanning for a workforce that is increasingly remote.

Overwhelmingly, when we begin work with a client, we find there is an incomplete understanding of where their assets are and what services are running on them.

With IoT, we are able to scan a large complement of IoT devices. We integrate with third-party solutions, such as network access control products that are not IoT intelligent, as well as directly with IoT products that are able to scan complex, advanced IoT devices like medical devices.

Knowing what you have to protect and what you need to protect is paramount for an efficient and effective vulnerability and risk management program. Organizations relying on ad-hoc scanning or not deploying a scanning solution to the entirety of their network are doing themselves a disservice and running the risk of introducing avoidable blind spots that could be detrimental to their network.

TAG Cyber: What role does exploitability play in vulnerability management and how do you incorporate that into Digital Defense's platform?

DIGITAL DEFENSE: It's unrealistic and impractical for an organization, regardless of how large or small their security staff, to address all vulnerabilities that exist.

Vulnerabilities that have been weaponized pose an exponentially higher risk than those that haven't or those that require more skill to leverage, even with the same severity ratings. Knowing the exploitability of a vulnerability allows security teams to focus their resources on those that pose the highest risk of compromise.

Exploitability is at the core of what we do, enabling organizations to focus their remediation efforts appropriately. Our Frontline. Cloud platform leverages the power of our proprietary machine learning model that incorporates over 20 threat feeds with multiple dimensions including exploitability and real-world-exploit use of vulnerabilities. This comprehensive data enables our clients to appropriately prioritize and properly respond to the most pressing emerging threats and attacks.

TAG Cyber: What are some of the common blind spots you see with enterprises?

DIGITAL DEFENSE: We see a few common situations that create blind spots for enterprises:

We see enterprises without a proactive, layered approach to security. Instead, they deploy a single technology, such as endpoint protection, and rely on the promise that it will prevent them from getting hacked. Unfortunately, nearly every organization that has been breached had some form of endpoint protection. Hackers know this and have many well-established techniques to maneuver around these protections. Understanding the true nature of your attack surface and employing a layered security approach can dramatically reduce your chance of a breach.

We also see enterprises scan only ad hoc or scanning only certain segments of the network and relying on other protections to cover the rest. Not having a centralized, accurate view of what exists leads to blind spots and potential points of compromise.

Finally, there are blind spots that result from asset scanning at different points in time. Networked computing assets may change their network characteristics, such as IP address, hostname, and even Mac addresses, due to normal business network churn caused by regular IT administration and maintenance of assets and the network. This poses a challenge for vulnerability management vendors and their ability to reconcile an asset that was scanned and assessed at different points in time. Vendors that struggle with this reconciliation mismatch scanned assets across time.

This results in duplicate assets in the vulnerability management asset view, or worse, a machine is mismatched to an incorrect machine counterpart across time. The vulnerability management solution declares vulnerabilities as fixed, when in fact they are not.

AN INTERVIEW WITH WITH JOHN LOUCAIDES, VP OF RESEARCH & DEVELOPMENT, ECLYPSIUM

SCALABLE DEVICE HEALTH BELOW THE OS

With phishing as the "low hanging fruit" on the cyber exploit tree, it's often hard for organizations to focus on lower level threats like vulnerabilities in hardware and firmware. Yet, the average enterprise has thousands of connected hardware devices running at any point in time, and each device contains myriad components that may be compromised anywhere along the supply chain—from build to ship to in-production use. Making matters worse, 99% of enterprise devices have known firmware vulnerabilities or misconfigurations, and over 80% have outdated firmware*. This creates an enormous attack surface which companies cannot afford to ignore.

While phishing might afford an easy entry into an organization's network, successful firmware exploitation affects deeper penetration more quickly. And because firmware can be harder and more complicated than software to update, business risk is high. Eclypsium helps companies defend against firmware attacks by finding and remediating weaknesses through scanning, threat detection, monitoring, and patch management. We spoke with John Loucaides, VP of Research & Development, about this growing problem.

TAG Cyber: How do firmware attacks differ from traditional malware attacks and network threats?

ECLYPSIUM: Unlike traditional malware and network threats, attacks that exploit the foundation of computing infrastructure can invalidate assumptions. This means that the normal techniques for detecting and responding to a problem may not work. That increases the level of access and the dwell time for an adversary.

TAG Cyber: With so many people now working remotely, how is device risk impacted?

ECLYPSIUM: Most organizations build up an expected risk profile based on a combination of physical and software-based controls. The move to remote work causes physical locations to go from the primary place of operation to more of a backup. As a result, both users and infrastructure may have more limited access to physical support. In this environment, device security becomes more important than ever.

TAG Cyber: The Nation Vulnerability Database has reported a rise in firmware vulnerabilities. How does this impact organizations as they manage an increasing number of devices (not just laptops/mobile devices) touching the corporate network?

ECLYPSIUM: Every device has dozens of components inside it that likely contain multiple firmware vulnerabilities. Unlike traditional OS and application vulnerabilities, most organizations are unable to monitor and track status at the firmware level. When dealing with an increased number and variety of devices that access corporate data, this attack surface explodes in size and complexity.

Unlike traditional OS and application vulnerabilities, most organizations are unable to monitor and track status at the firmware level.

TAG Cyber: What has your research lab observed in the last few months regarding exploits against device firmware?

ECLYPSIUM: Years ago, firmware attacks involved customization and targeting in order to mount a successful attack. Over the years, researchers proved that this was no longer necessary. Now, we're seeing more common attacks pivoting below the OS in order to bypass otherwise-effective security controls. Recent reports enumerated multiple in-the-wild bootkit attacks against the UEFI boot process. The US Department of Homeland Security (DHS) recently reported the same, indicating that device security vulnerabilities are being routinely exploited, especially in VPN equipment.

TAG Cyber: We hear a lot about "device health." What does that mean practically, and how does Eclypsium help?

ECLYPSIUM: Just like OS and application configuration and patch management, the firmware of each component inside a device needs to be managed. Unfortunately, organizations often don't have visibility below the OS, and even routine management activities quickly become complex and time-consuming when applied to device firmware and hardware at enterprise scale. This leaves devices exposed to a variety of risks.

In addition to security issues, reliability and performance often suffers as well. Recently, for example, firmware updates for enterprise systems have fixed issues related to battery performance** or data storage reliability***. Eclypsium delivers a scalable device health solution that helps organizations to manage and protect their fleet of devices down to the firmware and hardware level.

** https://eclypsium.com/product/ [*

*** https://pcsupport.lenovo.com/ca/en/solutions/ht508988/*

**** https://www.zdnet.com/article/hpe-tells-users-to-patch-ssds-to-prevent-failure-after-32768-hours-of-operation/*

AN INTERVIEW WITH WITH TONY PEPPER,
CEO & CO-FOUNDER, EGRESS SOFTWARE

MISDIRECTED EMAILS: THE MOST UNREPORTED SECURITY THREAT

Email is a business-critical communication tool. Even in recent years with the emergence and adoption of newer communication channels, email has kept its stronghold as the most widely used platform. With ubiquity, though, comes risk. Humans are so familiar and comfortable with email that we read and respond to most (non-obvious spam) email we receive. We send emails with attachments and links without thinking twice. And sometimes we send sensitive information. Even when we know we shouldn't. Because it's easy.

In cyber security, we think of email as a primary vector for compromise—but in terms of phishing, malware delivery, or other forms of attack directed at us. However, there is one area of email security that doesn't draw as much attention: inadvertent human error—accidentally sending email to the wrong recipient.

Yet it happens all the time. Sometimes it's innocuous, as in, "Wendy Cohen" received an email about an upcoming meeting that was intended for "Wendy Cohn." Sometimes, though, those misdirected emails contain financial data, PII, trade secrets, information about M&A activity, other types of information that require a much higher level of protection. This is where Egress Software can help. We spoke to Tony Pepper, CEO and Co-founder at Egress. about intelligent email security.

TAG Cyber: Egress has a message of "human-layer security." Why do you position your company this way and why is it important for better security?

EGRESS: Everyone we talk to says the same thing: the risk to email security has changed. Over the years, we've gone from implementing firewalls, MFA solutions, and encryption to anti-malware and DLP systems—but much of this technology has been geared toward keeping external intruders at bay. Traditionally, these technologies have been deployed at the network boundary and use static regular-based expressions to try to solve the problem. But they're unable to cater to the way we now operate, which has changed dramatically:

- We're all digitally connected more than ever via mobile devices
- We're working remotely now and for the foreseeable future
- The cloud has transformed the way we deliver services to customers

And, as we get caught up in this 24/7/365 working environment—becoming fatigued and rushing to get emails sent from our devices—all of this is dialing up the risk of a security incident happening when people share data via email.

Something we constantly hear from customers is that employees are becoming seemingly more "careless" in this environment; they end up sending more emails to the wrong person or with the wrong content attached; they send them without appropriate protection; and they even frequently fall prey to phishing attacks.

It means that people are now the dominant force

behind email security breaches. In fact, the UK's data protection regulator (the Information Commissioner's Office, ICO) recently published their incident trends for the start of 2020, and these findings show that misdirected emails and other human-activated data breaches are the most common causes for putting data at risk.

So, most breaches now are happening not because emails are being intercepted, but because of human-activated risks from inside the business that put sensitive data at risk. To handle this increase in human-activated risk, we see an opportunity for organizations to really evolve the way they protect themselves using human layer security technology.

TAG Cyber: Remote work has grown in popularity over the last decade, and, given recent circumstances, it's likely a higher percentage of office workers will continue to work at home even after it's safer to return to offices. How does this impact email security and access to sensitive data?

EGRESS: We've seen a 50% increase in email usage during the COVID-19 pandemic as a result of large-scale remote working, as people find new ways to communicate and get their jobs done. The upshot of this is that more sensitive data is being shared via email than ever before—widening the opportunity for a security breach to occur.

On top of this, the times people are sending emails has changed. The boundary between work and home has been completely eroded; people have been working from the living rooms and dining tables for months now. Some also have personal requirements, like childcare, brought about by social distancing. In response, people have flexed their work hours by working earlier or later than normal. Plus, they might be distracted in new ways by what's going on in the background at home. It makes it far more likely that employees are tired, rushing, stressed, and distracted—all factors that lead to people making mistakes and sending an email to the wrong person, attaching the wrong file, or clicking on a malicious link.

Finally, remote working has changed the devices people are using. A good proportion of employees are used to working on large monitors in the office environment. Sometimes they have multiple large monitors! Instead, many continue to work from laptops and utilize mobile devices. Smaller screens mean you're less likely to spot changes in the screen name when you're sending or replying to an email, meaning people are much more likely to accidentally populate an incorrect recipient name in the To/Cc field (often caused by autocomplete) or even reply to a targeted spear phishing attack.

It's consequently more crucial than ever that organizations deliver email security right to their end users, wrapping a safety net around them as individuals, to prevent incidents.

employees are tired, rushing, stressed, and distracted—all factors that lead to people making mistakes and sending an email to the wrong person

TAG Cyber: What is the extent of the misdirected email problem? Why do you think companies don't worry as much about it as they do other types of compromise?

EGRESS: We're only seeing the tip of the iceberg of this problem. Our research suggests that this is the most unreported security threat in any business; more than half of CISOs rely on employee reporting to track and mitigate insider data breaches, including misdirected emails—which is a big problem.

Firstly, and to give employees the benefit of the doubt, people have to realize when they've made a mistake in order to report it. Take sending an email in error—the sender has to check their sent items or receive a note back from a recipient before they realize that they've made a mistake. And then, the more complex part of the problem: Employee reporting is unreliable because people fear the consequence of having put data at risk. We read in the news about people being fired following breaches and know of horror stories from other organizations where employees are publicly named and shamed. So often, people may choose to let sleeping dogs lie. That's not to say there shouldn't be any consequences, but we need to ensure they're proportional to the intent behind the breach and do away with this blame culture around security incidents.

The upshot of this is that CISOs, understandably, don't have a clear picture of how frequently these incidents occur in their organizations. Normally, once we've investigated email data breaches for them, the problem is revealed to be between 15 - 20 times worse than they imagined; for one organization recently, it was 50 times worse.

Until you can quantify a risk, it becomes that much harder to dedicate security resources to tackle it, making it more likely that organizations will default to trying to mitigate longer-standing, more understood problems. Helping organizations measure the real risk of email data loss is one of our primary goals of our customer engagements—so they can see the tangible benefits of human layer security.

TAG Cyber: What interesting trends have you seen in terms of data loss or insider risk through Egress' research?

EGRESS: Our annual Insider Data Breach Survey compares the views of CISOs and IT leadership on insider data breaches with employees working in non-technical and non-legal remits. And the results are quite telling!

Our latest survey showed that 97% of IT leaders are concerned about insider data breaches, with 78% saying data at been put at risk accidentally in the last 12 months, and 75% saying it had happened intentionally. We also know that IT leaders are most concerned about the financial fallout of insider data breaches, with 41% saying this is their top worry when incidents happen.

At the same time, the survey shows how complex a problem this is. Only 29% of employees say they or a colleague have put data at risk accidentally and 32% saying they've done so intentionally. So, there's a clear disconnect between what IT leaders know is going on and what employees are willing to report— even in an anonymous survey! Part of this will be due to the reasons I mentioned earlier—employees might not know about incidents in order to report them or, more often than not, are afraid of the impacts. Our research has also shown there's a gray area when it comes to exploring employees' beliefs about who owns company data. Forty-one percent of survey respondents didn't believe organizations had any ownership over data generated or collected by employees, with the vast majority giving part or total ownership to the individuals or teams who worked on it. One-fifth of respondents (22%) felt that anyone within the organization had ownership over company data. This ownership muddies the water; people are more likely to take risks with data they believe they own, such as not using encryption when sharing it, and are also more likely to exfiltrate it, for example, when moving to a new job.

TAG Cyber: How do Egress' products differ from DLP?

EGRESS: First of all, we still see a critical role for traditional DLP technologies. However, we believe that alone it's not enough to mitigate this new generation of human-activated risk. Every conversation we have with security professionals ends up highlighting three concerns around existing DLP technologies:

1. It's not intelligent enough to prevent many accidental or malicious emails because it can't account for context

2. There's a lot of noise due to unnecessary alerts and false positives

3. The time spent on constantly updating policies gets in the way of productivity

Technology has evolved and we believe it can now more effectively support each individual user to keep data safe. What we do is overlay existing DLP policies with our contextual machine learning, that understands the email patterns and relationships specific to individuals, so that we can spot abnormal email behavior in real time and guide the user to prevent a security breach before it can even happen. And what that means is that we:

- Remove the risk of sensitive emails going to the wrong person or with the wrong content

- Minimize disruption and frustration at the user level

- Eradicate all that time that administrators would spend updating policy databases so it's a far more efficient process

AN INTERVIEW WITH WITH SHAI MORAG, CEO, ERMETIC

ELIMINATE EXCESSIVE ACCESS PERMISSION TO DRIVE DOWN RISK

Companies can no longer think about their networks in terms of inside vs. outside, as in, a network is a safe space that can be defended via some control or set of controls that keep internal resources protected and the bad guys out. In a perimeterless world, with the ubiquity of cloud and virtual infrastructures, companies must approach security with the assumption that everything on the network—no matter where it is—is potentially compromised. It is a continuous battle when the number of entities communicating on the network—applications, virtual machines, services, and processes—are constantly in flux.

In this world, the perimeter, insofar as it exists, becomes identity—the identity of what's communicating across networks. From people on devices to workloads, everything on the network has an identity, and that identity can be used to help security teams monitor activity and control access. We sat down with Shai Morag, CEO at Ermetic, to talk about how to secure workload identity and access, at scale, in the cloud.

TAG Cyber: Cloud has been around for a long time; why do companies still have access control issues?

ERMETIC: As the cloud matures, we see that the original security paradigms cannot be simply migrated to the cloud, they need to evolve or even be rebuilt from the ground up for cloud-native environments. Public cloud environments like Amazon AWS, Microsoft Azure, and Google Cloud Platform are complex ecosystems containing thousands of identities (human and machine), policies, and entitlements. We all know that it's important to limit access permissions and to enforce a least privilege model, but in IaaS/PaaS environments, it's very difficult just to get an accurate picture of the access permissions that are open to any identity.

Threat actors are well aware of this situation and that's why nearly all breaches involve excessive permissions to some extent. If you remove excessive permissions and enforce least privilege throughout the environment, you significantly reduce the attack surface.

TAG Cyber: what are some of the top cloud security concerns you see from cloud users?

ERMETIC: When we conducted a cloud security survey, we asked 300 CISOs about their top concerns associated with cloud production environments. They listed security misconfiguration (67%), lack of adequate visibility into access settings and activities (64%), and identity and access management (IAM) permission errors (61%).

In addition, 80% of respondents reported they are unable to identify excessive access to sensitive data in IaaS/PaaS environments. So, this is clearly an unsolved problem for most organizations.

TAG Cyber: Security configuration of the cloud is a priority for cloud users, but who in the organization is responsible for ensuring proper configuration and access controls?

ERMETIC: In cloud production environments, responsibility for security is shared between security, DevOps, site reliability and core cloud services teams. The majority of identities and permissions in IaaS/PaaS environments belong to infrastructure resources. So, the DevOps and cloud teams are the ones who create the policies and grant permissions. Security teams often lack visibility into these environments, so it's very important to bridge that gap. Both security and DevOps/SRE teams need full visibility into entitlements and understanding of the risks, and the ability to implement least privilege access across the board.

TAG Cyber: How does the Ermetic Cloud Security Platform work?

ERMETIC: Ermetic prevents cloud data breaches by automating the detection and remediation of identity and access risks in AWS, Azure, and Google Cloud. It automatically discovers all human and machine identities in the cloud and analyzes their entitlements, roles, and policies using a continuous lifecycle approach. By combining analytics with granular, full stack insight, Ermetic makes it possible to enforce least privilege access at scale, even in the most complex cloud environments.

Ermetic provides:

- Visibility: Discovers all human and machine identities, data and compute resources, policies and permissions, and provides a variety of visualization and data tools enabling you to understand relationships quickly.
- Risk assessment: Analyzes access policies to identify all entities that can access a resource, access logs to determine which permissions are used, and activity to model and identify risks while ensuring business continuity.
- Least privilege policy enforcement: Eliminates excessive access and privileges based on actual access patterns and data sensitivity to automate centralized least privilege policy enforcement.
- Anomaly Detection: Monitors access activities to detect and alert on suspicious behavior such as sensitive data access, privilege escalation and deletion, and unusual resource access.

80% of respondents reported they are unable to identify excessive access to sensitive data in IaaS/PaaS environments.

- Automation: Generates access policy recommendations for DevOps that optimize security while supporting end user productivity through integration with leading CI/CD tools such as Slack, Jira, ServiceNow, Jenkins, Terraform, and more.
- Benchmark audits: Performs routine assessment of configurations across cloud environments and automatically compares findings to your own enterprise policy rules or leading compliance benchmarks.

TAG Cyber: What's the one thing companies should do today to make their cloud deployments more secure?

ERMETIC: Eliminate excessive entitlements! According to industry sources, through 2023, 75% of security failures will be the result of inadequate management of identities, access and privileges. Today, identity is the perimeter so managing access is absolutely critical.

AN INTERVIEW WITH WITH JOHN DAWSON, PRESIDENT, EXACT DATA LLC

USING SYNTHETIC DATA TO SOLVE THE PROBLEM OF DATA OVEREXPOSURE

Data is essential to cyber security. From determining baselines in service of anomaly detection, to creating deception technologies, performance testing, and modeling, organizations need good data on which to make informed decisions. But when it comes to test environments for security vendor products, using real system data can be risky, cumbersome, and resource intensive. Further, advanced applications of synthetic data, like creating realistic honeypots based on behavioral attributes, haven't been sufficiently explored.

Synthetic data is not a new concept, but it's been slow to catch on in the cyber security space. Exact Data is changing that paradigm with its advanced algorithms and focus on the community. We spoke with John Dawson of Exact Data about how companies are starting to adopt and use synthetic data in their test environments.

TAG Cyber: In last year's Annual you explained the concept of synthetic data and how it can be applied in cyber security. Can you give us an update on what's happened in the space in the last year?

EXACT DATA: The technology application is gaining traction since last year! A major telecommunications company used our synthetic data for product development. They were having issues getting the necessary data from their technology partners on a weekly basis to maintain product development cycles. Not only was that problem solved, because they didn't have to wait for production data, but the company indicated that the synthetic data was better at speeding up the development process than anything else they have ever used.

Industry engagement has helped, too. Ixia's BreakingPoint network traffic generation product has exposed APIs and can now accept rich dynamic payloads. I would expect their competition to be following suit, including companies like Forinet FortiTester, Spirent Cyberflood, and Fireye. Interest has been high in areas such as testing for advanced behavioral threats and cyber range training, where the entire OS is simulated and enhanced with scenario-based events.

An interesting new strategy gaining attention within the cyber security community is using synthetic data for launching offensive misinformation campaigns. Misinformation campaigns involve generating synthetic databases that are indistinguishable from production databases and passing the information to adversaries, either through a

the fact that sanitized data in any form still contains private and confidential information that can be re-identified introduces unnecessary risk

honeypot deception solution or directly placed on dark websites dealing in selling stolen data. The result is that the adversaries will uselessly expend resources trying to sort out what is real and not, place doubt on any real information they might already have (if they can confirm it's real information), and run illicit fraud campaigns against people or scenarios that do not exist.

For example, the Boeing aircraft manufacturing company could leak synthetic, highly confidential wing design databases that, without extensive analysis or access to other information for verification, would be indistinguishable from the real ones. While threat actors could, potentially, gain access to Boeing's systems for research and analysis, it's far easier to use what they perceive as "leaked" on dark web sites.

Other examples would be if Equifax leaked bogus credit reports or if Visa faked personal financial information. The confusion and harmful effects on the adversarial community would be tremendous.

TAG Cyber: What challenges can the use of synthetic data solve for security companies?

EXACT DATA: There are a few fundamental problems synthetic data use will solve. The first is that the use of production data for development carries significant privacy and security risks, lacks an understanding of ground truth, and the developed products thus cannot be marketed, demonstrated, or trained on with the datasets used in the development process.

The second is that, without the use of synthetic data, security companies do not have a good way of scoring client safety—establishing some suite of products/tests/procedures that enables graduated scores for "certification of being fully protected." This certification process not only helps security companies better help their clients, but enhances their sales process and differentiates them from competitors. This type of scoring requires interactive and dynamic datasets that can only be created through a synthetic data generation process.

The third is that every company or government agency has had some sort of data breach at some point in time. They might not even know the breach has happened. Including an offensive misinformation campaign as part of the company's offensive cyber security strategy will mitigate damage from the "breach" and make that company a less attractive target once the adversary realizes they didn't affect the harm they were hoping for.

TAG Cyber: What are the benefits of using synthetic data versus using sanitized data?

EXACT DATA: Use of sanitized data is problematic because you are removing critical data elements necessary for testing; you have an unknown ground truth; you need to manually insert use cases. Also, the fact that sanitized data in any form still contains private and confidential information that can be re-identified introduces unnecessary risk and may mean that the company falls outside of compliance with data and privacy regulations.

TAG Cyber: What are some of the prevalent use cases, specifically amongst cyber security companies, you are seeing?

EXACT DATA: There are three general areas for synthetic data use: rich dynamic payloads for behavioral-based network testing and SOC operations, relevant sticky databases for deception/offensive solutions, and tagged training synthetic databases for AI/ML.

On the consulting side, security assessments that use synthetic data incorporate the recommended best practices of not using production data in development ecosystems and allowing enterprise to buy security solutions that have been tested and benchmarked. As an example, when purchasing a behavioral-based technology to detect online sexual harassment, the ability to test and score the system on how well the solution detects that company's specific policy use cases is critical. You don't want to end up with some generic solution.

TAG Cyber: How do Exact Data's algorithms help mimic the complexities found within most organizations' authentic data sets?

EXACT DATA: For synthetic data technologies, the challenge is not in the ability for algorithms to mimic those complexities, but in the ability to define them. Most agencies and clients we have encountered do not understand their data system of systems and business logic and workflow rules. Helping our clients define requirements and document data models, business logic, and workflow rules is our area of expertise. A side benefit is that we create documentation on their behalf, which is a necessary part of a robust strategic architecture and development roadmap.

AN INTERVIEW WITH WITH DR. MATT KRANING, CTO AND CO-FOUNDER, EXPANSE

PREVENT UNKNOWN AND MISCONFIGURED ASSETS FROM CAUSING AN EXPLOIT

Organizations' internet-connected ecosystems are constantly expanding. From on-premises data centers to public cloud, IoT to third-party systems, every entity presents an opportunity for attackers to achieve exploit. Preventing cyber attacks means understanding your organization's level of exposure, also known as the "attack surface." But defining the attack surface is more than merely learning which systems, applications, and the communication pathways between them are in your purview.

True asset management requires the added knowledge of all pathways to and from every asset, analysis of normal vs. potentially malicious behavior across communication channels, and how any one vulnerability could affect organizational risk.

We recently spoke with Dr. Matt Kraning, CTO and Co-founder at Expanse, a global digital asset management provider about how their platform helps organizations identify, track, and manage internet-connected operations infrastructure.

TAG Cyber: What do enterprises get wrong about asset management?

EXPANSE: Organizations do not understand the true extent or ownership of their internet assets, such as IP addresses, domains, and certificates associated with different systems and services. This leads to unknown and misconfigured assets causing unintended, public-facing exposures that represent significant business risk. Without a complete picture of the assets that make up their internet-facing attack surface, organizations cannot effectively defend their networks from malicious external actors.

Enterprises are more distributed than ever before, making it difficult for them to have a complete view of their assets. Business complexities that complicate asset management include:

- Mergers and acquisition events that introduce assets that aren't always properly inventoried, integrated, or configured
- Global subsidiaries and business units that don't always follow proper protocol
- Cloud migrations and instances of shadow IT
- Mobile workforces that inadvertently expose their laptops to RDP
- Strategic suppliers with which an organization shares sensitive data or permits network access

No single team owns the responsibility for finding internet-facing assets at most organizations, yet it's foundational to internet security. Various

asset lists exist in organizational silos and tools with many gaps between them.

Security teams then run their programs off of incomplete asset lists. Audits will look at vulnerability scan outputs to confirm that all critical vulnerabilities have been patched. But what about the systems that aren't scanned because they reside outside of the known network?

Further, some organizations don't even consider all types of internet assets they might own. They don't always inventory all assets that can introduce risk on the internet such as domains, IP addresses, certificates, cloud infrastructure, and even things like leased building HVAC controls.

These asset management challenges cause significant operational inefficiencies, as teams lose significant time manually tracking down and remediating assets, while still being blind to areas of exposure that could lead to serious financial and brand repercussions in the aftermath of a breach.

Organizations need to continuously discover all internet assets on-premises, in the cloud, or in consumer IP space by taking an outside-in view of every internet asset. They should integrate a single system of record for internet assets that is shared across their organization. And they should audit ownership and drive accountability for business-critical assets.

This will allow their operations and security teams to align with a common, current, and automatically-updated internet asset view across the business, improving governance and reducing risk. By automating the discovery and inventory of known and unknown assets, they will boost productivity and reduce costs. And by improving the speed of detecting and remediating security incidents, organizations reduce the likelihood of a breach and its associated costs and reputational damage.

TAG Cyber: Your product portfolio encompasses three phases of asset management: discovery, behavioral analysis, and link analysis. Can you explain why all three elements are important?

Expanse: Our three products solve different problems for different stakeholders in the organization:

Expander is focused on attack surface reduction and proactive management, and is typically sold to IT security teams involved in asset management or vulnerability management. Expander provides organizations with a complete, current, and accurate inventory of all public-facing assets. We believe that asset discovery is the crucial first step in both managing and reducing your attack surface. Without the ability to know what

Many organizations rely on supplier self-attestation or risk scores to assess supplier risk, but there are many insufficiencies with these approaches.

assets are yours, your enterprise will always leave gaps that attackers can use to compromise the network. Expander helps automatically discover these risks without requiring any agents or instrumentation.

Link enables organizations to proactively monitor for security risks within their strategic suppliers and drive remediation. Link provides similar discovery capabilities to Expander but with a specific eye toward an enterprise's supply chain and other third-party risks, and is focused more on evaluating the security posture of an organization by looking for risks instead of being a central system of record for a company's own assets. It is typically sold to teams that focus on supply chain risk management.

Behavior is a network policy enforcement solution and is most commonly sold to network security teams. It models enterprise network security policies and uses global internet traffic data to detect deviations where parts of the network are not consistently and correctly implementing organizational policies. These gaps could allow attackers to bypass network security controls and compromise the enterprise. With Behavior, organizations can monitor for policy noncompliance across their ecosystem and drive enforcement through Behavior integrations and open APIs. While having strong security policies is important, they mean nothing if they are not implemented consistently across the enterprise. Behavior empowers organizations to identify areas of noncompliance with policy and drive policy enforcement.

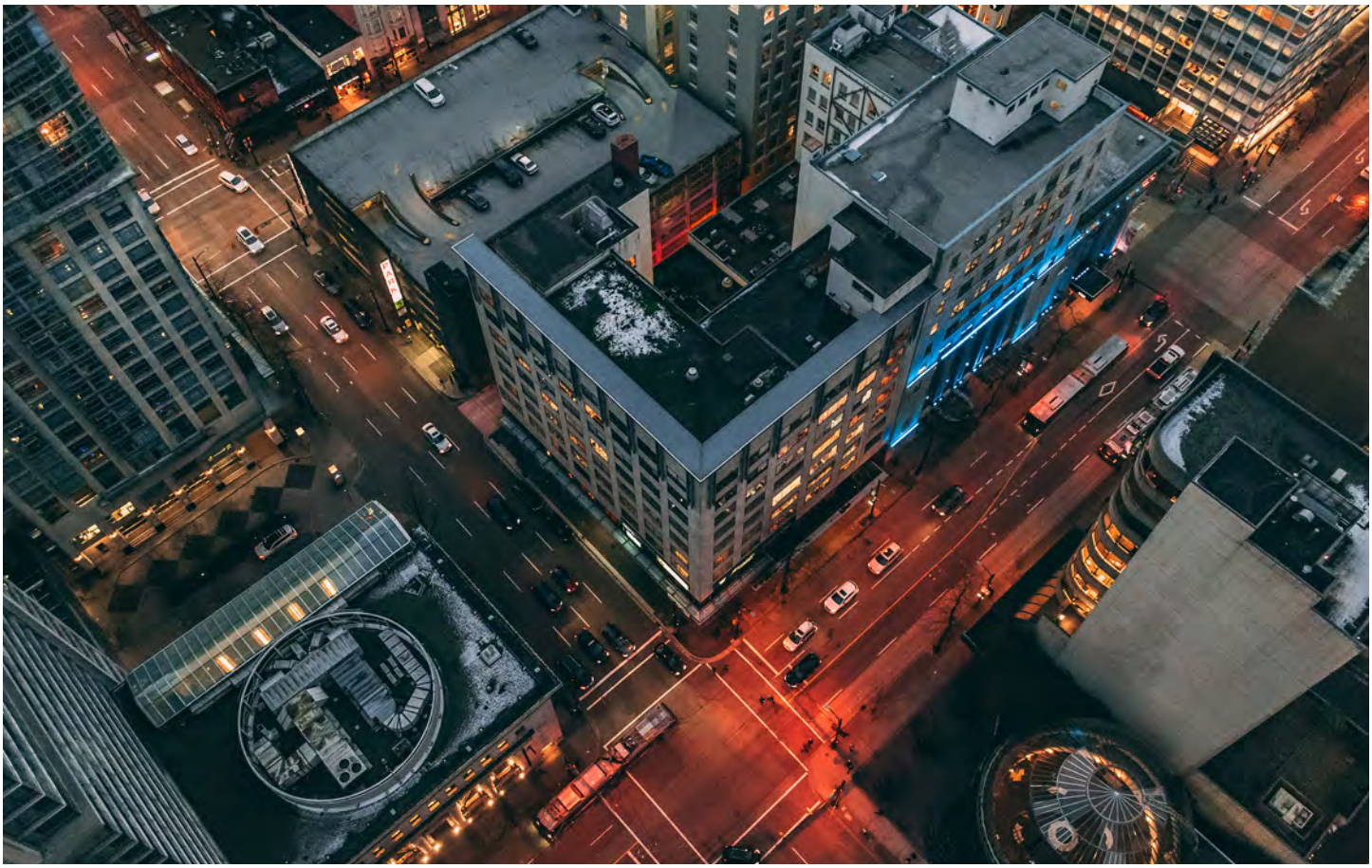
Of these products, Expander is the one that is most relevant for asset management.

TAG Cyber: How do organizations' supply chains—their 3rd party connected ecosystems—affect how they discover and manage cyber risk?

EXPANSE: Organizations today can no longer concern themselves only with the traditional enterprise perimeter. Most large organizations work with an array of third-party suppliers and partners. These third parties can then introduce complexities for IT infrastructure teams to account for and add new challenges for cyber security teams to manage. Strategic suppliers are sometimes given privileged access to corporate network services and data but don't always have the same security resources that the parent organization does. Attackers know to go after weak links in the supply chain and then pivot to more valuable targets. Many organizations rely on supplier self-attestation or risk scores to assess supplier risk, but there are many insufficiencies with these approaches.

TAG Cyber: A large part of asset management is monitoring for indicators of compromise, but Expanse doesn't use risk ratings as a guide. Why?

EXPANSE: Risk scorers/risk ratings/security ratings are known for having high false-positive rates, relying on stale and inaccurate data; have low data refresh rates; and cannot meaningfully predict breaches. Expanse provides real-time, advanced asset discovery using our ML-based attribution engine and has an extremely low false positive rate. Expanse's tech stack helps organizations continuously monitor strategic suppliers for cybersecurity risks and noncompliance. This enables Expanse customers to prioritize the riskiest suppliers and drive meaningful operational change in suppliers' security practices.



AN INTERVIEW WITH WITH
JONATHAN NGUYEN-DUY, VP,
GLOBAL FIELD CISO TEAM, FORTINET

ADVANCING SECURE NETWORK DIGITAL TRANSFORMATION

A clear and powerful trend in modern enterprise computing and networking is the advanced support now required to enable digital transformation. This drive comes from the highest levels of the organization, often with direct involvement from boards and CEOs. For technical teams, this creates challenges, particularly for security, but also opportunities to improve how the business performs its day-to-day functions toward near- and long-term goals.

From a security perspective, the primary requirement involves enablement—and this means creating solutions that allow the business to address the great IT themes that support digital transformation. These include multi-cloud hosting, mobile device integration, software-oriented implementation, and more recently, work-from-home initiatives using virtual tools.

We recently had the opportunity to spend some time with Fortinet's Jonathan Nguyen-Duy, Vice President, Field CISOs. We asked Jonathan how the Fortinet platform enables network digital transformation through advanced security protection.

TAG Cyber: Let's start with the threat landscape. What are some trends you're seeing at Fortinet?

FORTINET: We're seeing a consistent expansion in variety, velocity, and sophistication of threats—from automated, opportunistic attacks to highly targeted campaigns. The pandemic has presented new opportunities for threat actors; the first half of 2020 demonstrated the dramatic scale at which cyber criminals and nation-state actors leveraged a global pandemic as an opportunity to implement a variety of cyber attacks around the world. The adaptability of adversaries enabled waves of attacks targeting the fear and uncertainty in current events as well as the sudden abundance of remote workers outside the corporate network, which quickly expanded companies' digital attack surfaces overnight.

Although many compelling threat trends were related to the pandemic, some threats still had their own drivers. For example, ransomware and attacks targeting Internet of Things (IoT) devices and operational technology (OT) are not diminishing; they're evolving to become more targeted and sophisticated.

At a global level, many threats are seen worldwide and across industries, with some regional or vertical variation. Similar to the COVID-19 pandemic, a certain threat might have started in one area but eventually spreads, meaning most organizations can face the threat. There are, of course, regional differences in infection rates based on factors such as policies, practices, or response.

At the same time, we see many of the

recurring, systemic cyber security issues, such as vulnerability management, misconfiguration, human errors, and security awareness, especially in light of the shift to remote working. Lack of multi-factor authentication, data black up, privilege access management, and other simple-to-intermediate controls continue to be problematic.

With growing threats against IT and OT infrastructure, the threat landscape is far more complex than ever before. Threat actors are using AI and automation to detect and exploit gaps in visibility, integration, and automation.

TAG Cyber: Your team talks often about supporting digital transformation. What's the role of secure networks in this area?

FORTINET: DX initiatives are transforming enterprise networks characterized by new solutions and operating environments, such as IoT devices, cloud-based data storage and applications, mobile devices, and new branch locations. Many of these new devices have unique vulnerabilities, such as the use of default manufacturer credentials in IoT devices and cloud deployments' use of infrastructure outside the organization's control.

In organizations of all sizes, users/entities, devices, and applications are moving outside the traditional network perimeter, creating new security complexities and risks. For example, a business continuity scenario necessitates a more remote workforce while the drive for seamless access, data-driven decision making, accelerated revenue recognition, and enhanced experiences is driving cloud adoption—resulting in hybrid networks. The emergence of new network edges means that security has to be applied on the LAN edge, WAN edge, and cloud edge, in flexible consumption options from appliance-, VM-, or cloud-delivered services. The rapid growth of secure SD-WAN is evidence of the need for integrated security and networking—to ensure holistic security and WAN management for optimal performance for an enhanced customer experience. It's clear that business outcomes and customer experiences can only be achieved if security and networking are working in a broad, integrated, and automated manner.

Contactless commerce and remote working will be standard operating models requiring highly distributed networks characterized by 5G performance and reliability.

As networks grow more complex and hybrid, organizations require a broad, integrated, and automated security platform to simplify and optimize incident detection, prevention, and response. This enables visibility across the entire digital attack surface and the ability to reduce security complexity and speed operations and incident response. Addressing these new risks and attack vectors requires the convergence of security and networking —what Fortinet calls Security Driven Networking.

TAG Cyber: Can you tell us about some of the new capabilities offered as part of the Fortinet solution suite?

FORTINET: Fortinet continues to focus on innovation and performance value. This is seen in the release of our latest hyperscale network firewall. Today's most digitally-innovative organizations face escalating and often unpredictable capacity needs that are quickly outpacing their security solution's performance capabilities. The hardware acceleration via purpose-built NP7 network processors of FortiGate 4400F delivers the first single compact appliance with security performance and scale.

We've also launched Fortinet Secure SD-WAN for Multi-Cloud, which is a new approach to establishing secure and high-performance connectivity between public cloud workloads running on multiple clouds without increasing cost and complexity. Available in all major cloud providers, this enables a consistent network architecture leveraging SD-WAN capabilities between clouds and empowers application developers and enterprise IT to build a high speed and seamless cloud-to-cloud network and security architecture.

In addition, we continue to expand our Fortinet Fabric Partner Program, with over 360 technology integrations—ensuring adaptability with legacy investments and best-in-class technologies. Fortinet's open ecosystem provides integrated solutions to customers for comprehensive end-to-end security. The Fortinet Fabric-Ready Technology Alliance Partner Program brings together a community of global technology partners with specialized expertise and makes available resources and tools to facilitate integration.

TAG Cyber: I see that you've recently acquired OPAQ. Can you tell us about the rationale and plan for integration?

FORTINET: Fortinet has been driving zero trust network access (ZTNA) and SASE convergence across devices and cloud-based solutions. The OPAQ acquisition provides great flexibility to offer security on the SD-WAN edge, data center edge, and cloud edge. Fortinet's combined with OPAQ's patented ZTNA solution enhances Fortinet's existing SASE offering to form the best-in-class SASE cloud security platform with the industry's only true zero trust access and security by providing industry-leading next-generation firewall and SD-WAN capabilities, web security, sandboxing, advanced endpoint, identity/multi factor authentication, multi-cloud workload protection, cloud application security broker (CASB), browser isolation, and web application firewalling capabilities.

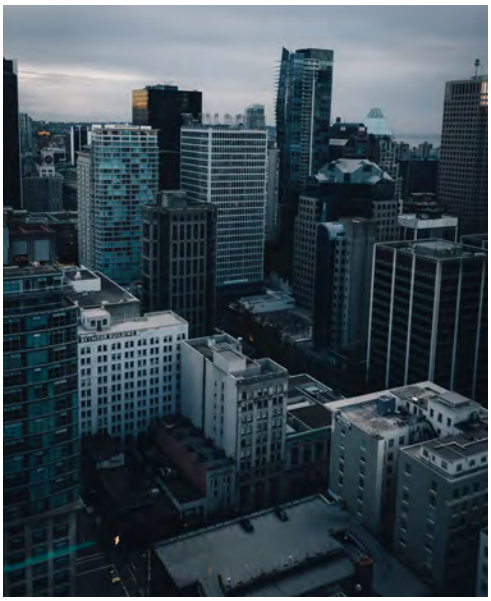
Moreover, OPAQ's platform is built to be partner friendly, empowering MSSPs, carriers, and partners to easily integrate the SASE multi-tenant platform into their own offering and add value to business and government customers with OPAQ's NOC and SOC professional services.

Given remote workforce requirements, with exponentially more users, devices, applications, services, and data outside a traditional enterprise edge, the integration of Fortinet's broad Security Fabric with OPAQ's cloud platform will offer customers and partners even more choices in how they can consume security and is yet another way Fortinet is empowering customers with integrated security and networking innovation in real time.

TAG Cyber: What's been your observation about how the global pandemic has affected or influenced the way networks are operated and secured?

FORTINET: The pandemic accelerated many of the macro trends in terms of borderless networks, accelerated networking, and greater complexity. Driven by business requirements and the need for seamless access to resources, networks are now much more hybrid and distributed across remote locations, the traditional enterprise perimeter, and multiple public clouds. This results in security requirements that support hyperscale, highly distributed networking from the LAN edge, WAN edge, and cloud edge. In essence, businesses need highly effective security at speed and scale.

The shift to remote working and edge-based computing has driven the acceleration of ZTNA controls, ensuring that all requests for network access are identified, authenticated, validated, logged, and monitored. The challenge is how to accomplish this across millions of simultaneous connections



without sacrificing performance. Performance is key because security that doesn't keep pace with business requirements rapidly becomes irrelevant.

Going forward, contactless commerce and remote working will be standard operating models requiring high distributed networks characterized by 5G performance and reliability. The resulting security requirements will center on broad, integrated, and automated solutions powered by AI. In addition, networking and security will be more integrated to ensure better business outcomes and enhanced experiences.

TAG Cyber: Any predictions about future cyber threats and how technology companies will provide solutions to mitigate risk?

FORTINET: Digital transformation has driven mass adoption of cloud solutions and greatly expanded the attack surface. Distributed application development without integrated security often leads to vulnerabilities. These factors, along with greater complexity in computing, networking, security, and compliance, often lead to gaps in visibility, awareness, and control. Cyber criminals and nation-state threat actors have access to the same AI, automation, and other tools as defenders, and use those tools to detect and exploit the growing number of vulnerabilities.

There is no question that cyber attacks and threats are here to stay, but they are also becoming increasingly sophisticated and dangerous. Cyber criminals are eagerly adopting AI and automation via AI fuzzing, self-learning swarm-based attacks, and expanded malware-as-a-service capabilities. If that weren't bad enough, year after year we still see that most vulnerabilities exploited were known and patchable.

So, I think cyber threats will only grow to be even more problematic and destructive, especially ransomware. Today's and tomorrow's solutions must be able to identify, authenticate, validate, log, and monitor all traffic, as well as determine the final disposition of data that was accessed. This has to be done at speed and scale across millions of simultaneous connections.

AN INTERVIEW WITH WITH IAN PRATT, GLOBAL HEAD OF PERSONAL SYSTEMS SECURITY, HP INC.

BUILDING THE MOST SECURE PCS IN THE WORLD

The modern PC remains one of the primary staples of enterprise support for day-to-day accessing and creating digital content, for browsing, interaction, research, communication, management, sales, document production, and just about every activity in support of business and government. As such, managing security of PCs and other devices in the office and the home, like printers or other collaboration devices, is a top-of-mind concern for most executives and practitioners.

We recently had the great opportunity to connect with Ian Pratt from HP to learn more about how his team is developing and supporting world-class cyber security solutions for enterprise customers. The discussion covered several general areas of technology and future cyber threats, as well as an overview of specific product offerings from HP. Here is a brief digest of our conversation:

TAG Cyber: Thanks for sitting down with us. First of all, can you help us understand the distinction between HP and HPE? I suspect there might be some readers who could use a brief refresher on the corporate set up.

HP: The separation of Hewlett Packard Company in 2015 created two separate, more focused publicly traded companies: Hewlett Packard Enterprise and HP Inc. Today, HP Inc. has market leading positions across personal systems, printing, and 3D printing. As a standalone company, HP has invested in innovation and built a high-performance, purpose-driven culture that has enabled the company to outperform its markets. This includes an industry-leading position in endpoint security, with the world's most secure PCs and printers.

TAG Cyber: Let's start with PCs: Can you provide a brief overview of the specific types of controls that are being embedded into HP products to avoid threats?

HP: HP believes that with the evolution of cyber-threats every PC purchase decision is a security decision, meaning that security requirements should be clearly considered when making a technology choice. HP has been innovating for over two decades to create industry-first and differentiated security solutions that are built into our devices. These solutions are present below, in, and above the OS and protect the device, OS, applications, and data. Our security-by-design approach for PCs starts with the hardware, where we have our unique HP security controller chip built into all commercial PCs, functioning as the

root of trust and enabling us to ensure the system boots from a secure state and then monitor changes. Our aim is to deliver an architecture that can not only offer protection but provides resilience too. It's with some pride we can claim the title of "The World's most Secure and Manageable PC."

TAG Cyber: What has been your experience with printer security? Do enterprise teams get hacked through their printers?

HP: Printers are one of the most ubiquitous IoT devices in both homes and offices. Strong printer security has become essential for organizations of all sizes as various white hat and malicious exploits have shown the ease with which legacy printers could be compromised and used as vehicles to get access to sensitive company assets. It's important to make sure that printer firmware is kept up to date, that unused features and exposed protocols are disabled in configuration, and that printers are connected to appropriately segmented networks. HP printers make use of some of the same "security chip" technology used in HP PCs, and many of HP's printers and MFPs come with unique layered security features that can detect malware and self-heal without IT intervention. For peace of mind and time savings, many organizations, with or without dedicated IT security staff, are actively seeking out Managed Print Services to have this all taken care of by experts such as HP's Print Security Advisors.

Various white hat and malicious exploits have shown the ease with which legacy printers could be compromised and used as vehicles to get access to sensitive company assets.

TAG Cyber: I've heard your team reference isolation as a primary strategy for offering security protection. Can you give us an overview of your advanced isolation technology?

HP: A key capability of the HP Security stack is the creation of a zero trust endpoint architecture from the hardware up. In addition to designing our machines so that each layer of the stack, starting from the hardware, can protect, monitor and self-heal the next, we also now deliver cyber resilience for end user activity using a scalable virtualization-based application isolation technology. We can seamlessly create individual virtual machines (not software enforced sandboxes, but true virtual machines) that create a slice of the hardware, firmware, and OS to be used by a particular user task or application. The application is contained within this limited privilege virtual machine and does not have the ability to access users' data or applications sitting within the host environment. Therefore, even if malware executes within such a virtual machine, it will not have the ability to do any harm—there's nothing of value to steal or corrupt, and no ability to propagate. The user can simply close the application window or browser tab and the virtual machine is disposed of along with the malware. We call this the ability to "protect without detection," which offers radically better protection than any detection-based approach.

TAG Cyber: What sorts of threats do you see hitting enterprise customers in the coming years? Will PCs and printers be targeted increasingly by nation state actors?

HP: Increasingly, bad actors are financially motivated. The size of the cyber crime industry is huge and is threat actors are becoming increasingly more organized and effective at what they do. There is now a whole supply chain of criminal organizations specializing in different steps of the attack kill chain, in business together to maximize yield from campaigns. There's also evidence that criminal organizations are increasingly taking a more long-term view rather than making quick ransom demands, so some should be classed as advanced persistent threats along with traditional nation-state actors.

Endpoint systems are very much at the frontline of cyber defense, with over 70% of enterprise breaches starting with an endpoint compromise. Almost invariably the compromise comes from tricking a user into clicking on something and is perhaps even more likely to happen with users working from home without the benefit of enterprise network protections or colleagues to consult. We need our endpoints to look after themselves, to protect users from bad clicks, and that's why this is such an area of focus for HP, why application isolation is such a game changer.

AN INTERVIEW WITH WITH GEORGE AVETISOV, CEO AND CO-FOUNDER, HYPR

WHAT'S A PASSWORD?

Passwords continue to be a top contender for the title of Top Initial Access Point in Cyber Security Breaches. It's, perhaps, a dubious distinction, but one that has perpetuated for well over a decade. While cyber security practitioners bemoan the use of passwords and have been dreaming up ways to replace them for years, the industry is only now starting to see more fervid enterprise adoption of passwordless technologies. The advantages of doing so are obvious: stronger, multifactor authentication that can't be easily spoofed or stolen by threat actors.

While some businesses are reluctant to give up passwords for fear that employees will encounter friction, legacy password-based solutions also face adoption issue—and have resulted in only incremental authentication gains. Passwordless is truly the future of authentication, and companies like HYPR are showing how passworldess authentication can actually reduce the friction associated with validation of identity plus reduce the risks and management costs associated with passwords. We spoke with George Aveitsov, CEO and Cofounder at HPYR, about the passwordless movement.

TAG Cyber: When people hear passwordless, they might automatically assume some sort of futuristic, biometric-based scanning to validate identity and authorize access. Can you help clear up some of the misconceptions about what passwordless is?

HYPR: Ah yes, the old question of passwordless marketing vs. true passwordless MFA.

This was a misconception much earlier on in the passwordless transformation. People realize now that there is a difference between a passwordless user experience and true passwordless MFA. These days security teams know that simply enabling Touch ID or Windows Hello with your identity provider does not eliminate your password problem. As such, passwordless has become its own pillar of authentication, with some analysts breaking it out from "legacy IAM" into its own category.

In fact, this is indicative of a larger trend. We are witnessing a rapid decoupling of authentication from identity.

Over the past decade, identity has become more centralized, while authentication has become more fragmented. Now as the cloud wars rage on, Microsoft, GCP, and AWS are rapidly commoditizing third-party identity providers. In an effort to reduce the user disruption and identity turmoil of the cloud transformation, more and more businesses are focusing on user authentication. Passwordless technology has made it possible for these businesses to decouple authentication from the identity layer. There is a growing trend towards decoupling and why it's happening now, and HYPR is delving into how business leaders are using passwordless to accelerate their cloud transformation.

TAG Cyber: What are some of the more common scenarios that are well-suited to passwordless authentication?

HYPR: We do extensive research on adoption with our customers and partners, which we publish in an annual list of the Top 10 Passwordless Use Cases.*

Among the leading use cases are:

DESKTOP MFA: IT leaders are solving the #1 gap in corporate access by enabling true passwordless MFA for workstation login. This has been a huge issue for years as corporate IT teams wrestled with the added friction of adding MFA to workforce login. A sharp rise in the number of remote workers, plus the friction of complex password requirements has brought this use case to the forefront of passwordless adoption.

PASSWORDLESS RDP: With RDP attacks at an all-time high, and remote login a #1 use case in the Covid-19 era, this has quickly become a top use case. Passwordless RDP is enabling admins and remote workers to emulate smart cards to enhance the user experience.

STRONG CUSTOMER AUTHENTICATION: Specifically across financial services, the customer MFA gap has been a huge issue for years. With passwordless authentication being embedded in consumer-facing applications, this is now leading to huge reduction in fraud rates. CVS Health, for example, saw a 98% reduction in account takeover fraud by going passwordless. That is an astounding percentage.

TAG Cyber: From a tactical perspective, what would it take for an enterprise to replace passwords? How hard is the human transition vs. the technical one?

HYPR: From experience in deploying passwordless to thousands of employees and millions of customers, our perspective is as follows:

The human transition is not the challenge. Your users are already using passwordless methods on a daily basis

The human transition is not the challenge. Your users are already using passwordless methods on a daily basis. Between Touch ID, Face ID, and Windows Hello, most of your user base is experiencing passwordless authentication regularly. You're not changing their behavior; you're actually playing catch up. The technical transition is pretty straightforward. Like any enterprise-grade product, it is important to put deployability, scalability, and ease of use at the forefront.

The real challenge? It's the enterprise mindset that has to change. Many organizations don't even realize they can go passwordless, much less what that actually means. We once saw a company deploy passwordless MFA to their workforce and enforce smart cards—meaning, employees could no longer use a password to log in. Several hundred users were told they could forget their password completely. Except no one thought

ahead to some of the infosec folks who proceeded to have a quarterly phishing and password awareness training session. A few confused employees and clarifying emails later, the session was removed from employee calendars. It's now a standing call for other infosec awareness training.

It's really fascinating observing when an enterprise realizes it is finally reducing the use of passwords. It's like they're waking up from The Matrix for the first time.

TAG Cyber: The FIDO Alliance is the leading industry association focused on stronger authentication standards. What is HYPR's relationship to the Alliance, and how does that translate into you're the solutions you offer?

HYPR: HYPR is a board member of the FIDO Alliance, alongside industry leaders such as Microsoft, Google, Mastercard, and Bank of America, so we help contribute to the standard. We are also part of the User Experience steering group.

We have been huge believers in the standard and contributors since our founding in 2014. The passwordless transformation would not be possible without the widespread adoption of FIDO standards. Open standards such as SAML, OAUTh, and TOTP have helped drive the IAM industry forward. With FIDO we, as an industry, are able to finally deliver on the passwordless vision.

As a member we have contributed directly in technical and user experience. We have also driven public awareness, education, and large-scale adoption of FIDO. CVS Health, for example, has more than 10 million passwordless users deployed and is a vocal advocate of the FIDO impact.

Personally, I think HYPR is strongly committed to educating the public on the impact and nuances of FIDO through great content such as our popular FIDO Buyer's Guide. Another widely praised guide is FIDO vs. MPC, where we explored the comparison of FIDO against multi-party computation, an alternative approach to passwordless authentication.

TAG Cyber: Security practitioners have been cheering on the passwordless revolution for years. Is it really coming? If you had a crystal ball for future authentication, what would it show?

HYPR: The passwordless revolution is not coming, it's already here. It was Bill Gates who famously proclaimed the password officially dead in 2004. He suggested that "smart cards are the way forward."

He was right, just way ahead of his time.

The technology has just finally caught up with the vision. The passwordless transformation needed 3 key things to happen:

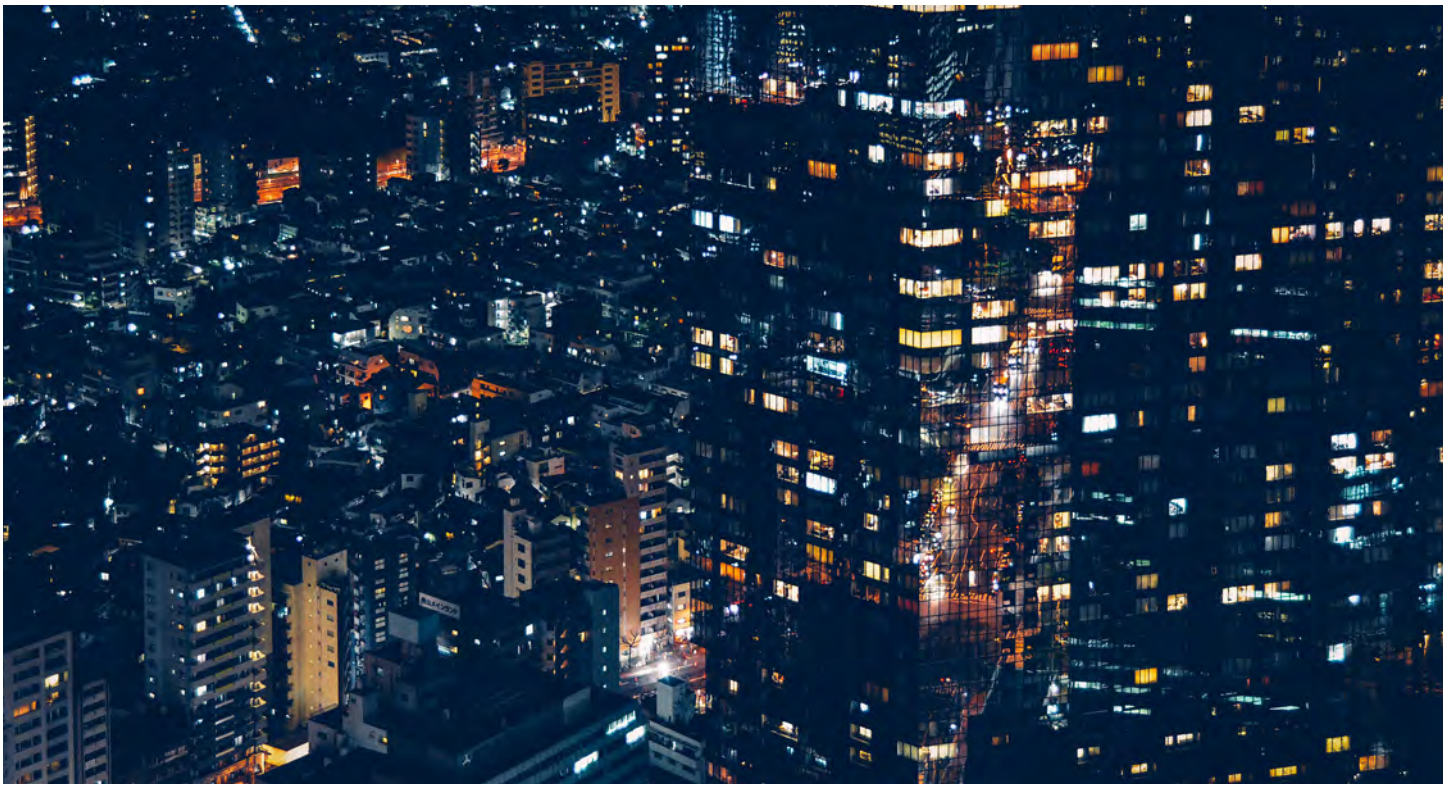
1. Smartphones
2. Mainstream adoption of biometric authentication
3. Open standards for passwordless authentication such as FIDO

A true passwordless solution enables you to use your smartphone as a smart card or a FIDO token. The convergence of these trends in just the past five years has opened the floodgates for widespread adoption of true passwordless authentication. Some analysts have forecasted that by 2022, more than 60% of enterprises will have adopted passwordless methods.

Bill called it ten years before we did. When we started HYPR in 2014 we knew the passwordless decade was coming. With trends like this it doesn't matter who is right; it matters who is at the right place at the right time.

At HYPR we have dubbed 2020 the start of The Passwordless Decade. Our prediction is that by the end of this decade, schoolchildren will be asking their parents, "Mom, Dad - What's a password?"

** https://www.hypr.com/top-10-passwordless-use-cases/*



AN INTERVIEW WITH WITH KUNAL ANAND, CTO, IMPERVA

INTEGRATING RUNTIME SECURITY TO APPLICATIONS

For many years, the only reasonable option to address run-time security issues in an application was to install a traditional web application firewall (WAF). While early WAF technology remains a powerful means for detecting anomalies and evidence of breaches, security solutions have had to evolve to meet the needs of more modern, complex software applications running in myriad different configurations including hybrid and multi-cloud operating environments.

The preferred approach to protecting applications today is more holistic, and uses data, analytics, and a multi-layered architecture based on WAF, DDOS security, API security, bot protection, and run-time application self-protection (RASP) to address dynamic risks. These different controls support a woven defense that can be used to secure applications, regardless of their design, hosting, or configuration posture.

We had the opportunity to speak with Imperva CTO Kunal Anand, one of the world's leading experts in application security. As one of the principals of Prevoty (acquired by Imperva in 2018), Kunal has had the benefit to participate in the evolution of application security and RASP protection in particular.

TAG Cyber: Let's start with the concept of a WAF, since this is so closely associated with Imperva. How has traditional WAF technology evolved to a more modern solution?

IMPERVA: Imperva has continuously challenged our thinking of WAF. When we started 18+ years ago, WAF was just an on-premises appliance. Today, both on-premises and cloud WAF are commonplace.

For our cloud WAF, we've created what we call a "single-stack" approach. We operate a global, unified network of more than 45 points of presence (PoP), where we offer DDoS protection, WAF, advanced bot protection, API security, and client protection all in the same control flow/stack. All our PoPs run these capabilities to stop very large attacks against our customers.

To continue evolving, we invest heavily in research and development. Our threat research team is constantly on the lookout for the latest exploits and is shoring up our capabilities before our customers even notice. We incorporate our data, investigating more than 1T requests and stopping more than 20B application attacks every month.

We're really excited about our WAF roadmap; we've been bridging application and data security—specifically, incorporating capabilities like data discovery and classification. Trying to protect data access at the edge is something our biggest customers ask us about, and we'll continue investing there. Other areas we're pursuing involve user-to-data access, which touches compliance and privacy, as well as leveraging identity for zero trust.

TAG Cyber: You have particular expertise in an area known as runtime application self- protection or RASP. Can you tell us how this works?

IMPERVA: The simplest way to think of RASP is that it protects applications from the inside out whereas WAF protects applications from the outside in. Today, AppSec isn't just about closing out vulnerabilities, although it's an issue all organizations have to face (per Veracode, it takes an average of 150+ days to fix a critical vulnerability). It's about protecting a vector that attackers are using to access sensitive data. From industry analysis, the top 10 application and API breaches resulted in more than 1B sensitive records breached, which is more than direct database exfiltration. In the most recent NIST draft, RASP is included in the framework as a control to help with detection, protection, and response.

By attaching to a runtime, RASP can provide more context than other technologies. Of course, it's up to the vendors, and not all RASP solutions are created equally—some stay at a surface level, looking at things like HTTP requests and stopping there. While that might solve for a particular set of attack classes, it misses the real intention of RASP, which is to look into a wide vector of security issues that AppSec teams have to face on a daily basis. When my co-founder and I built Prevoty, the RASP solution acquired by Imperva in 2018, we broadened our approach to provide in-depth protection for attacks like SQL injection, command injection, network access, weak cryptography, and many more.

the top 10 application and API breaches resulted in more than 1B sensitive records breached, which is more than direct database exfiltration.

Some of the largest organizations in the world have been able to deploy RASP in production at a significant scale—from large banks, to financial services, to retailers, to telecommunications organizations. For them, they've been able to recognize ROI through the reduction in remediation efforts as well as having a zero-day safety net within the application.

TAG Cyber: I've heard you reference something called LANGSEC. Can you explain?

IMPERVA: Today, lots of security technologies focus on using signatures and pattern matching via regular expressions to look for things like SQL injection. Ultimately this type of defensive model can fall short, as they have to be constantly revised to account for newer offensive breakthroughs.

More than a decade ago, some very smart researchers created a different approach to analyzing and understanding payloads in a security context, which they called LANGSEC (Language Theoretic Security). Instead of using something like a regular expression to look for SQL injection attempts, what if you could actually parse a query the same way that query planners in underlying databases work to understand what the query actually contains? It turns out that

LANGSEC is more accurate and efficient (parsing the query once + running checkers against a parse tree) than running hundreds, and sometimes even thousands, of regexes against the content.

Our RASP product implements LANGSEC in conjunction with a positive security model to prevent broad classes of attacks like cross-site scripting, SQL injection, remote code execution, command injection, lateral networking, and more. On top of delivering great performance, it gives application security teams greater confidence.

TAG Cyber: How should an enterprise combine WAF, DDOS security, and RASP into an integrated application security approach?

IMPERVA: I believe that, when it comes to production AppSec, we must focus first and foremost on protecting critical assets while shifting attacker economics. While the former is obvious to CISOs, the latter is just as important. The more resilient we can make the entire application stack—from the perimeter all the way through the application runtime—means that an extremely large number of attacks should be mitigated, prompting individuals wielding automated scanners and tools to seek different targets.

In terms of practicality, I would frame this as a defense in depth-oriented approach encompassing the following three items.

- DDoS protection is all about stopping large volumetric attacks at the edge. It's not just the number of packets—it's also the size of each packet. To stop it effectively, you need a global presence and a unified global network. To stop DDoS while being compliant, you have to deal with stopping attacks as far out as possible (to save precious compute and data resources) while allowing clean traffic into specific regions/countries that adhere to privacy laws and regulations.
- WAF is about wholesale investigation and analysis at a perimeter. While WAF is still important for protecting against the OWASP Top 10, its use cases have broadened to cover API security, bot protection (account takeover, scraping, etc.), client-side protection, and traffic manipulation, all based on very advanced rules.
- RASP is about protecting applications at runtime, which means that it can see into code flow execution in a way that you can't at the perimeter. Specific classes of attacks include remote code execution, non-trivial classes of SQL injection, and more. From our data, more than 52.7% of application security attacks are targeting vulnerabilities in the application stack to perform command execution. RASP can help close this gap plus others. For us, we've found a way to combine them together—to enrich requests from the WAF to RASP and to have RASP provide more context if it stops an attack back to WAF, to try and stop attacks at the edge.

By putting these three pieces together, organizations can push themselves into a stronger position for protecting applications and the data behind them.

TAG Cyber: What are some thoughts you might have on API security? This appears to be a growing concern for CISOs.

IMPERVA: This is a pressing issue for CISOs and CIOs. Across the board, organizations are deploying more APIs than your usual front-end application, and it makes sense; APIs are reusable components that tend to focus on business functionality.

Unfortunately, these APIs are just applications, which means they bring along all the baggage of a traditional application and suffer from vulnerabilities as well. The problem with APIs is that they're typically one layer up from of data stores that contain sensitive information, which means that they touch both security and compliance teams.

When it comes to API security, I advise CISOs and CIOs to break down the problem into five questions. In order, they are:

1. Where are your APIs (north-south and east-west) and do you have something beyond a basic API gateway to protect them?
2. Where are your API schemas and are you comfortable with the input/output going over specific endpoints?
3. In a production system, who's accessing specific endpoints?
4. How much sensitive information is being accessed by external/internal users?
5. Is the access normal/abnormal?

These questions aren't designed to stump a CISO/CIO—they're designed to guide them to start decomposing the problem and answering the more important areas asynchronously.

TAG Cyber: Any predictions about application security in the coming years you might share? Will artificial intelligence, for example, be an important part of this equation?

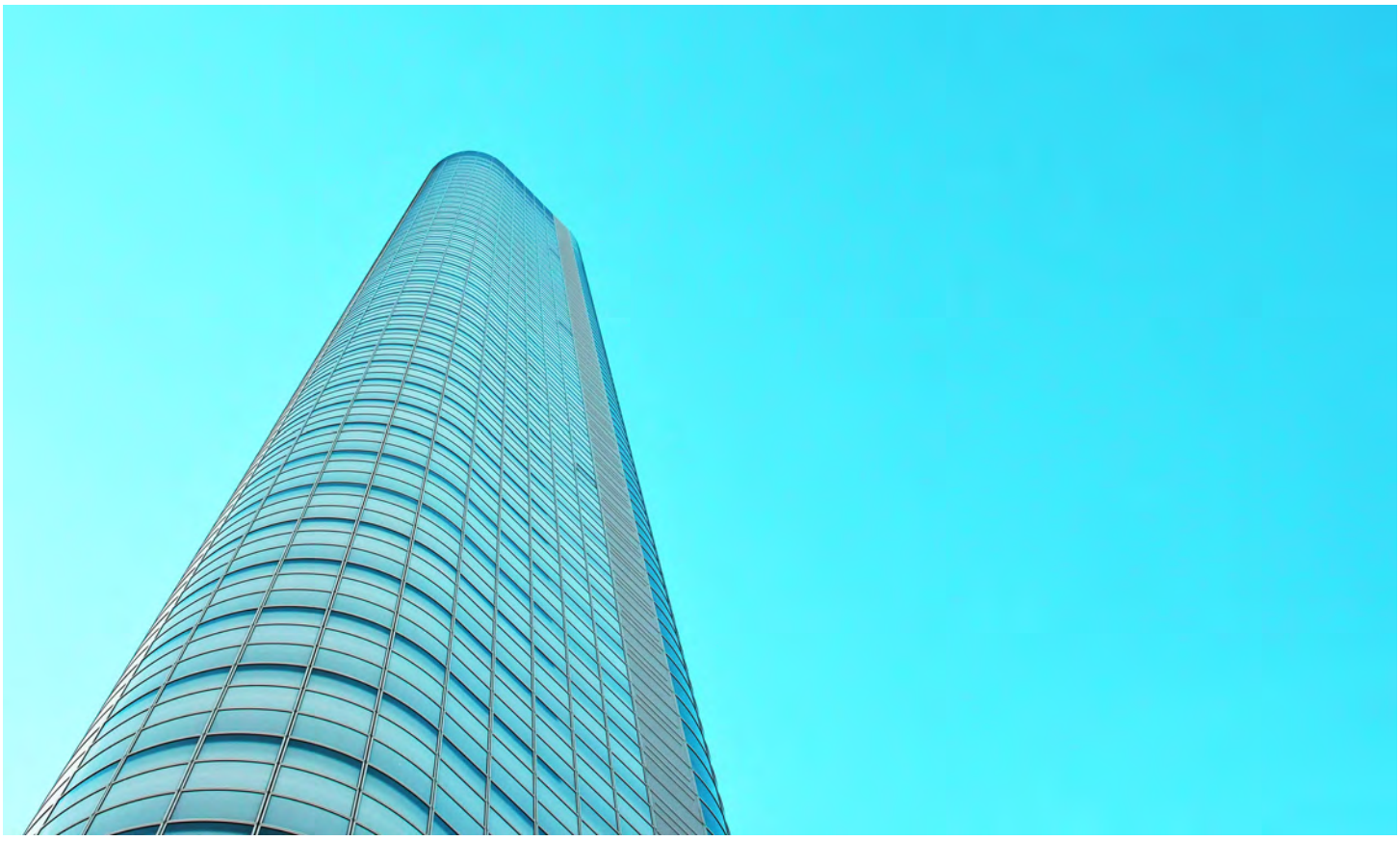
IMPERVA: I love speculating about AppSec! Here are my predictions, in no particular order:

1. We're going to see vendor consolidation and compaction in the space. There are too many vendors in AppSec and there's a lot of overlap with very little differentiation. If you look at companies like Imperva, it's only natural to continue adding capabilities—organically through R&D and inorganically via acquisitions (Incapsula, Prevoty, Distil, etc.). I think we'll see more "single stack" plays emerge; expect to see some best-of-breed rollups. I can also see application and data security coming together to solve specific use cases like user-to-data access monitoring.

2. I think we're on the cusp of seeing some really novel attacks hit the mainstream. I've connected with three-letter agencies around some creative and disruptive AppSec attacks that have targeted all aspects of the CI/CD process (IDEs, open source libraries, etc.). At the same time, I've seen interesting implementations of machine learning that generate highly sophisticated payloads designed to circumvent defenses like regex-based signatures.

3. With GPT-3 by OpenAI making the headlines recently, I imagine that we'll see similar technologies in security. I can see AI being used offensively (see point 2) as well as defensively. I can imagine something like GPT-3 looking at other source code and automatically rewriting vulnerable/weak code to be stronger while preserving business logic.

4. Programming languages will become more resilient to security attacks. Languages like Rust offer stronger runtimes and attempt to offer security by default. And, they've found a way to allow developers to be extremely productive while eliminating many annoying classes of runtime issues/errors that typically set off language scanners.



AN INTERVIEW WITH WITH DR. ABRAHAM GILL, CHAIRMAN AND CEO, INCYBER

AUGMENTED INTELLIGENCE TO MANAGE INSIDER RISK

Insider risk has emerged as a top-three concern reported by enterprise CISOs. It's no surprise, given that insiders require authorized access to corporate resources. Insider risk is not a straight-forward problem. Insider threats can arise from unintentional mistakes made by well-meaning employees; insiders can be targeted by external actors for use of their privileges; or a disgruntled employee might purposely abuse privileges to harm the company, seek revenge against a perceived corporate enemy, or exfiltrate data and secrets for personal gain.

Mitigating insider risk requires a sophisticated approach to identifying advanced indicators of compromise via threat intelligence and user behavioral analysis (UBA). Monitoring and analyzing patterns of behavior can reveal evidence of attempted or successful malfeasance and provide opportunity for security and operations team to prevent further destructive behavior.

InCyber, Inc. utilizes the core tenets of UBA—access to evidence, processing capability, and action-oriented output—to enable organizations to effectively defend against insider risk. Here, Dr. Abraham Gill, Chairman & CEO, InCyber, Inc., shares insight to current trends and mitigations.

TAG Cyber: Data is everything in an enterprise. Tell us about InCyber's data collection and processing.

INCYBER: InCyber is user centric and the focus is on user activities as well as external parameters such as integrity, credit score, gambling addiction, etc. We only need five parameters from a client's database—user ID, time stamp, description, filename, and path to the filename—to start the process of identifying threats and providing the evidence to our clients.

TAG Cyber: UBA is often considered a detection and response capability, yet you talk about InCyber as an early warning system. Can you explain the differences between traditional UBA and your method?

INCYBER: InCyber provides augmented intelligence. This is quite different than UBA. We combine internal information and internal log data with legally obtained external telemetry collected from our customer, such as eCredit rating, integrity information, legal status, and more. UBA doesn't do that, and the way we correlate data allows us to create intelligence the enterprise can act upon and deter potential high-risk employees, contractors, or consultants. Using the aforementioned type of external data to augment the accuracy of our results leads to 10X fewer false positives than traditional methods.

In addition, our processing algorithms are designed to use advanced heuristics to identify common threads, meaningful relationships, and subtle connections in the data, which means that InCyber can proactively detect potentially bad activity weeks or months ahead of insider threats, thereby reducing clients' risk.

Millions of employees are now on leave without pay but still have access to the company infrastructure

TAG Cyber: Why is an agentless deployment an important element of your product?

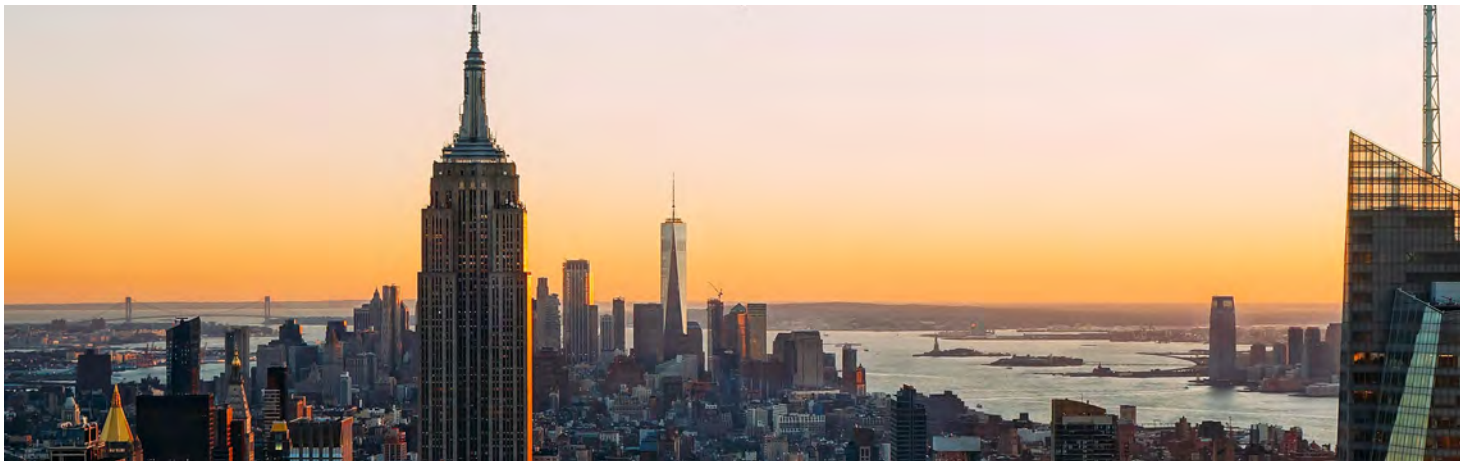
INCYBER: Agents make the users very uncomfortable, plus there is the problem of agent fatigue. Instead, we save time and money by extracting user activities from the database or wherever they are stored by the client. The platform is designed to collect and ingest data that is already present—even finding evidence that may have been previously undetected by other systems—which is why InCyber is such an easy tool to deploy and integrate.

TAG Cyber: Are you seeing any alarming or notable trends in insider risk?

INCYBER: Unfortunately, COVID-19 and the resulting work-from-home climate caused a substantial increase of insider activities, including malicious theft as well as impersonation of credentials. Bad actors took significant advantage of the fact that their employers weren't ready to migrate all users to insecure working locations, leaving systems and access less protected than they would be if all employees were on-premises. Plus, the crashing job market left many employees disgruntled and/or stressed. Millions of employees are now on leave without pay but still have access to the company infrastructure—they get to keep their system usernames, user IDs, and passwords—which makes them potentially very dangerous. Combined with the chaos of the pandemic, this is a perfect storm for insider attacks.

TAG Cyber: If organizations could do just one thing (aside from deploying InCyber!!) to mitigate insider risk, what would you recommend?

INCYBER: The most important thing is to collect all the activity logs and restrict access to sensitive data. You can't do anything about potential threats if you're not watching what's going on in your enterprise. Doing this manually is a monumental task, so implement automation.



AN INTERVIEW WITH WITH TED SHORTER, FOUNDER AND CTO, KEYFACTOR

ADDRESS YOUR CRYPTO MESS WITH AUTOMATION

Digital keys and certificates form the backbone of public key cryptography. However, as the amount of digital exchanges has increased over time, managing certificates and keys has become an arduous task that often gets shoved to the back of security practitioners' priority lists. Doing so, though, puts companies at risk of compromise. Numerous security incidents have been facilitated by expired certificates, missing signatures, insufficient validation, and more. With the increase in cloud usage, DevOps, and IoT all affecting how certificates and keys are managed, companies need easier ways check for and remediate issues.

PKI (public key infrastructure) often gets painted as outdated and hard to use, so automation is an imperative for any system of key/certificate management today. Keyfactor offers enterprise PKI-as-a-service. The company starts by helping customers understand the scope of their PKI and certificate management problems, then deploy tools and managed services to ease their pain. We spoke with CTO and Founder, Ted Shorter, about end-to-end cryptography.

TAG Cyber: What are some of the legacy complaints about PKI?

KEYFACTOR: There's an annual report we do every year with the Ponemon Institute that highlights some of the core complaints around managing PKI. One main problem is that companies don't have the right IT and InfoSec people who have expertise in PKI. Around 53% of organizations are unable to hire and retain enough qualified IT security personnel with expertise in PKI. Shifting IT resources, coupled with a decline in the number of PKI and cryptography experts in the industry, have left most PKI deployments shorthanded.

Organizations also tend to think of PKI certificates as they relate to SSL/TLS. They hyper focus on SSL/TLS certificates used for internet-facing or internal applications. However, SSL/TLS management is only a fraction of the certificate landscape. Cloud services, containers, and service meshes all use machine-to-machine communications that rely on client authentication certificates. Many outages are not caused by expired SSL server certificates, but by a failure to track web service client authentication certificates.

It takes just one to slip through the cracks, yet 74% of IT and security experts believe their organization does not know how many keys and certificates they have, much less where to find them when they expire.

TAG CYBER: What are some of the current market trends affecting PKI and cryptography?

KEYFACTOR: While some tend to paint PKI as outdated, it's actually being used more than ever. An estimated average of 88,750 keys and certificates are used by organizations today to secure data and authenticate systems.

Migration to the cloud requires significant changes to key and certificate management practices. Most companies embracing DevOps are using certificates to secure containers but are less confident in their ability to scale PKI across on premises data center, cloud, and hybrid environments.

The largest trend for PKI is in IoT device identity provisioning and management. When you hear that there will be 25 billion connected "things" by 2021, that immediately raises the question: "How are they secured"? Not only do companies need to embed security during the design and manufacturing state, but they also need to think through how to update that security if it has a certificate.

TAG Cyber: Proliferation of certificates doesn't seem to be slowing, especially as everyone shifts to work from home. Where does PKI fit in?

KEYFACTOR: You're right that certificate usage and expansion won't be slowing anytime soon. PKI is a double-edged sword if not properly conceived and planned. Most PKI out there today is not designed to go beyond the traditional network of the four walls of the organization.

Organizations' current state PKI isn't designed to scale to the cloud and does not have those capabilities built in to reach where the data lives. It can't be "just protect the things that are in my four walls" anymore. PKI can be leveraged, but the scale must be built in or the PKI must be reconsidered to address the scale.

TAG Cyber: Speed and high assurance can be at odds. How does Keyfactor tackle that challenge?

KEYFACTOR: If you architect a solution from the ground up, knowing that speed will be a requirement, then speed and high assurance won't be at odds. The challenges we see with our customers is that they're using legacy architecture and technologies to solve next-gen problems and initiatives.

Around 53% of organizations are unable to hire and retain enough qualified IT security personnel with expertise in PKI.

With our PKI as-a-service, they don't have to worry about the speed and scale. For example, a customer in the automotive manufacturing space couldn't maintain this duality of speed and scale with their current solution. One of the requirements we had to prove out in our POC was the ability to scale certificate issuance and renewal across 500 million+ devices. That's a lot of devices! Even though they didn't have the many, they wanted to stress to load and scale of our solution to make sure we could future proof any expansion needs that would need.

TAG Cyber: If a customer starts with a crypto mess, isn't it still a massive undertaking for them to get started on your platform?

KEYFACTOR: The first step is to get an inventory of what you must understand to address the mess. We have scanning, discovery,

and monitoring tools that can scan your entire network beyond your SSL/TLS certificates to find them. We show customers how easily we can do this and they're blown away at how quickly we identify every crypto asset on their network. And this isn't a one-time thing; we continuously scan to pull in any certificate that maybe issued without their knowledge.

After that, naturally, comes assignment of maturity levels to enable automation and agility. This includes processes like:

- Defining automation and approval workflows for certificate issuance, provisioning, renewal, and revocation
- Identify high-priority applications for certificate automation (e.g., web servers, load balancers, etc.)
- Aligning with DevOps' priorities and certificate usage practice

Our platform is designed to keep pace with the growing number of cryptographic keys and digital certificates to decrease operational costs. Many security teams still struggle to deploy and manage certificates using a patchwork of manual spreadsheets, internal PKI, and CA-provided tools. However, keeping up with certificate renewals isn't enough to stay ahead anymore, as evolving cryptographic standards are now challenging enterprises' ability to respond and adapt.

AN INTERVIEW WITH WITH ANN JOHNSON, CORPORATE VP OF SECURITY, COMPLIANCE, AND IDENTITY BUSINESS DEVELOPMENT, MICROSOFT

IMPROVING PRODUCTIVITY AND COLLABORATION THROUGH INCLUSIVE, SECURE USER EXPERIENCE

Cyber security is filled with thousands of small and medium-sized security vendors, all offering a slice of the security pie. When you look at the more limited list of behemoth security vendors, you'll notice a pattern: many started by offering one security or security-adjacent product and grew through a series of product add-ons and/or acquisitions.

Such is the case with Microsoft, hardly a security company when it was founded in the late 1970s but now hard to ignore as a leading provider in 2020. Today, Microsoft offers security solutions across four broad areas: Users and devices, data and apps, threat protection, and infrastructure. For most other security companies—in an industry where niche startups often dominate conference halls—any one of the aforementioned functional areas would be a product in and of itself. But over the last 5 years, Microsoft has been making a big play to be the all-in-one provider, both through internal development and acquisition of best-of-breed products. We recently spoke with Ann Johnson, Corporate VP of Security, Compliance, and Identity Business Development at Microsoft, about what the current cyber security landscape and industry trends.

TAG Cyber: Normally, you travel extensively, speaking with security teams all over the world. What topics are forefront in CISOs minds today?

MICROSOFT: With massive workforces now remote, the stress of IT admins and security professionals is compounded by the increased pressure to keep everyone productive and connected while combatting evolving threats, many of which are now leveraging the global pandemic.

My conversations with CISOs have revealed that heightened security concerns and cost reduction measures are needed as they have had to navigate and adapt to this new world of enabling secure remote work.

Among the questions I'm hearing from our customers;

- How do I quickly and securely get a newly mobile workforce connected when, where, and how they want to be productive?
- What new threats are being generated and how do we stop them?
- How do I help employees to practice good security habits during a crisis?

TAG Cyber: How has widespread remote work changed how CISOs have to approach their security strategy?

MICROSOFT: When billions of people formed the largest remote workforce in history, overnight, we learned much more than how to scale virtual private networks. We were reminded that security technology is fundamentally about improving productivity and collaboration through inclusive end user experiences. This is a huge paradigm shift for our industry. By providing security tools that are empathetic of someone's situation—and forgiving of mistakes— people are protected, and blockers to productivity are removed.

This is an approach we at Microsoft call Digital Empathy, and it actually empowers people to work when, where, and how they need, and use the devices and apps that maximize their productivity.

TAG Cyber: Microsoft is a high-value attack target given your breadth and depth; how does the company balance providing best-in-class technologies with the perception that you're "always under attack"? How does that affect your strategy and messaging?

MICROSOFT: A second paradigm shift we are also seeing is the greater adoption of a zero trust philosophy.

Zero trust is an "assume breach" security posture and treats each step across the network and each request for access to resources as a unique risk to be evaluated and verified. We saw zero trust shift from a business option to a business imperative in the first 10 days of the pandemic. Looking past the pandemic, we expect that zero trust architecture will become the industry standard.

We were reminded that security technology is fundamentally about improving productivity and collaboration through inclusive end user experiences.

TAG Cyber: How are you building in zero trust to the various Microsoft product offerings?

MICROSOFT: Zero trust is based around 3 principles: First, verify explicitly, use least privileged access, and assume breach.

We continue to invest in making Azure AD a comprehensive identity solution that securely connects employees, partners, and customers to any app they need, from any location, on any device. This means expanding the app ecosystem, deeper integrations with popular apps, and providing new tools to connect non-standard legacy applications. We want to make it easier to manage identities and access through deep integration with cloud systems and cloud provisioning.

Zero trust security relies heavily on pervasive threat signal and telemetry. It's essential to connect the dots and provide greater visibility to prevent, detect, and respond to distributed and

sophisticated attacks. Microsoft Threat Protection covers M365 workloads across identity, endpoints, data, and applications; Azure Security Center protects all workloads and applications across Azure, on-premises, and Azure Sentinel, our cloud-native SIEM.

TAG Cyber: What areas will Microsoft Security be focusing on as we head into 2021?

MICROSOFT: Our goal is to meet customers where they are today, so they are able to look past the pandemic. To do this, we are responding to these challenges in a phased approach. First, we needed to help our customers manage their crisis response.

The next phase, as we look past the pandemic, will be about recovery and helping customers do more with cloud security. We must do this while also looking for ways to streamline customers' security and save money. Looking forward, we will help them reimagine new opportunities for growth, securely.

Increasingly, we see convergence in the areas of security, compliance, and identity, in terms of both customer needs and the role of security decision makers.

AN INTERVIEW WITH WITH DAN SLOSHBERG, SENIOR DIRECTOR OF PRODUCT MARKETING, MIMECAST

EMAIL SECURITY BEYOND THE PERIMETER

Email is the ingress for a disproportionate number of cyber attacks. Phishing, spam, and malware are pervasive, and secure email gateways (SEGs) are a front-line defense in the effort to block and quarantine suspicious emails before they hit users' inboxes. SEG controls, in turn, reduce the potential for a user will clicking on a bad link, opening an infected attachment, exposing credentials, or otherwise providing unauthorized entry to valuable system resources.

If email presents the most prevalent attack surface, the web isn't far behind. Astute attackers know that fake websites with malicious content or those designed to steal user information are a reliable exploit mechanism. Companies need security solutions that can identify and block malicious sites, inspect content and file downloads, and enforce granular policies at the gateway.

Together, web and email protection provide security control at a "new perimeter"—the front door to companies' systems. Mimecast offers solutions for email, web, and data to identify high-risk entities and stop attacks before they reach the internal network. Dan Sloshberg, Senior Director, Product Marketing at Mimecast, spoke with us about rising threats against email and web.

TAG Cyber: What are some of the more alarming trends you're seeing related to attacks against users via email and web-based properties?

MIMECAST: Cyber threat actors and threat groups are continuously researching and testing new attack methods to exploit increasingly diverse and decentralized business processes and apps, and they're therefore circumventing sophisticated defenses. The forced explosion in remote working has caused greater complexity and increased risk for many organizations. Unfortunately, threat actors have "followed employees home," using a variety of attacks designed to exploit the situation and users' vulnerability, to obtain personal and confidential information.

Mimecast's State of Email Security Report 2020 shows insights on the latest attack trends, while the 100 Days of Coronavirus report looks at the impact of the pandemic itself. The data confirms the perfect storm the pandemic has created, with all security detection rate categories reviewed increasing by 33% on average from January to end of March 2020. Spam, impersonation, and malware detection are all up, but malicious URL clicks saw the biggest spike at 50 percent.

This confirms that attackers are using a combination of email and web attacks to achieve compromise. They have started setting up fake login pages to steal credentials for popular web-based collaboration services and then send a phishing email to encourage visitors to click through to the site.

The net-net is that attackers are relentless, making security strategy and approach more important than ever.

TAG Cyber: The idea of a perimeter is long gone, but you talk about a new perimeter of sorts, one that includes email gateways, the web, and access inside the network. Why is this multi-layered approach more effective than traditional single-point controls?

MIMECAST: Mimecast Email Security 3.0 is Mimecast's strategy to help IT and security professionals achieve a more comprehensive form of protection against email and related attacks by advancing from perimeter email security to a comprehensive, more pervasive approach. This approach addresses threats in three distinct zones: at the email perimeter, inside the network and organization, and beyond the perimeter.

At the perimeter: Attackers send spam and viruses via email and embed URLs in email to conduct phishing and spear phishing attacks. They also deliver forms of malware that organizations can't detect with signatures and traditional antivirus technologies. Impersonating trusted senders continues to grow in scale and sophistication. With over 90% of attacks coming via email and the ever-growing volume of messages that come in and go out of an organization's perimeter, it's critical to concentrate security controls at the gateway.

Inside the network and organization: Threats that exist inside an organization are often underestimated and unseen, which means they also carry a lot of risk. Attacks can spread silently and rapidly from user to user or, even worse, from employees to customers and partners. Without adequate security awareness, end users are susceptible to making an innocent but devastating mistake. Our focus is detecting and preventing the lateral and outbound spread of malicious links, weaponized attachments and sensitive information, and raising employee's security knowledge and vigilance.

Beyond the perimeter: Brand impersonation attacks that exploit an organization's good name to compromise customers and partners are devastating. They destroy trust, are extremely difficult to uncover, and are even harder to shut down. Unfortunately, they're all too easy for criminals to create. Even unsophisticated attackers can simply register similar domains and host websites designed to trick unsuspecting visitors, damaging the brand equity it may have taken you years or decades to build.

Essential steps for prevention include implementing DMARC to protect the domains you own, while also proactively hunting for and remediating attacks that spoof your website to steal information and money from your customers, partners, and supply chain.

Across the perimeter: Complex security challenges often lead to complex security ecosystems—a reality reflected by the fact

Spam, impersonation, and malware detection are all up, but malicious URL clicks saw the biggest spike at 50 percent.

that organizations are using numerous disparate technologies to address their security needs, with some companies using as many as 75 different deployed solutions. Making it all work together is about more than optimizing investments. It's about correlating telemetry and intelligence and sharing it across resources so they can all work more effectively.

TAG Cyber: Human error facilitates many cyber attacks today. How can organization realistically control attack progression in the face of stolen credentials and compromised accounts?

MIMECAST: The harsh truth about awareness training, according to Mimecast's Customer Tech Validate Survey 2019, is that $1.5B is spent on security awareness training and yet 64% of employees are unenthusiastic about it. Time and time again, awareness training is not engaging, and attendees are not paying attention or they aren't learning the right things to do. This can create a dismissive attitude towards security. Security awareness training that positively shifts a culture need to be engaging, frequent, and provide consistent context.

The key to awareness training is employee engagement coupled with detailed risk analytics that help companies monitor and benchmark results. Training should be fun and interactive, not just a test to see if someone can pass.

TAG Cyber: Brand exploitation is an increasing concern in a world of disinformation. How do attackers conduct these attacks against brands and what can victim companies do about it?

MIMECAST: Attackers are increasingly using your brand as bait, launching lookalike websites to trick your customers, partners, and wider supply chain into divulging credentials, sensitive information, and even handing over money. These attacks are often invisible and put your brand and reputation at risk.

Unfortunately, conducting these attacks is simple and quick. An attacker can register a similar domain to yours, scrape your website including login page, and initiate a targeted phishing campaign targeting your customers, suppliers and others that trust your brand.

To help guard against these brand exploits, organizations need to extend phishing protection beyond the email perimeter to proactively uncover and take down attacks at the earliest stages. Solving this requires a combination of automated web scanning; analysis of key indicators of compromise, including new domain registrations and security certificate issuance; tracking of website cloning; the ability to identify unknown attack patterns; and the ability to identify and block compromised assets at the earliest preparation stages before attacks become live.

AN INTERVIEW WITH WITH JJ CRANFORD, SR., PRODUCT MANAGER, OPENTEXT ENCASE

CONTENT MANAGEMENT AS A SECURITY BENEFIT

As digital transformation continues, organizations are faced with protecting increasing amounts of business-critical data and content. Data has long been considered the "crown jewels" of an organization, and security teams rely on solutions that secure access to data, control rights for data use, and encrypt data so its value to attackers is diminished when and if they do manage to access data repositories.

The balance between data/content security and ease of use is a growing concern; security teams can't infringe upon employees' abilities to use data, yet unfettered access increases risk. As such, security professionals need technologies that provide full visibility and control of data—from endpoint to server—and allows for rapid identification and remediation of data-centric threats, all while facilitating authorized, secure access.

OpenText was founded as an information management company and has since evolved to include information security services as market trends pushed data management and data security closer together and similar needs were echoed in the customer base. We spoke with JJ Cranford, Senior Product Manager at OpenText EnCase, about the information management space and how it collides with cyber security.

TAG Cyber: The security business at OpenText grew out of customer and market demand. Tell us about your strategy for growing OpenText's security business.

OPENTEXT: After OpenText became an enterprise security provider, it made quite a bit of sense to align products within our own ecosystem that could add value to both data management and security. OpenText is a leading provider of content management systems like Documentum™, InfoArchive™, and others, and these content repositories are often the source of cyber security threats because the sensitive files stored in those locations are the ultimate target for cyber attackers. Bringing security closer to the content itself leads to the ability to monitor and address late-stage cyber breaches—which is a win for our customers.

TAG Cyber: Where are the biggest holes in organizations' enterprise content management security strategies today?

OPENTEXT: The siloes between records management and security are substantial. Records managers don't often think about the data world through the lens of cyber security, as that role is more about uptime, access, and authentication. A typical information security team would be focused on hash values or SIEM alerts, and they are less likely to approach security from a file contents perspective. The ability to answer questions like these can lead to added security effectiveness – "What machines or users have access to a high amount of sensitive data? What are the contents of the

It's all about the combination of technology and human behaviors, not one or the other or one over the other.

files that are sensitive? Who is accessing these files? Are there unusual patterns around time of access or amount of data interacted with? Are suspicious regions or geolocations involved in access to sensitive content?

TAG Cyber: Beyond the obvious centralization of data, why are content management systems such juicy targets for cyber criminals?

OPENTEXT: The ultimate goal of most cyber attacks is to access sensitive data and exfiltrate that data for later monetization—meaning that content repositories are a proverbial gold mine for adversaries. Cloud sources and content repositories are notoriously difficult to monitor, with most approaches focusing on monitoring data as it ingresses and egresses the content repository itself. Valuable contents, in addition to the lack of security and control in traditional content management systems, create a perfect storm for bad actors to initiate compromise.

TAG Cyber: In your experience, how common is it for organizations to not know the extent or sensitivity of their content and data, and why does that matter?

OPENTEXT: We have seen improvements in recent years, but organizations still have a ways to go in terms of understanding the contents of files for security use cases. Aside from the issue of external hackers, insider threats represent a substantial area of risk to a business. Credentialed users that choose to act nefariously and abuse access to sensitive data do so in ways that are difficult to monitor.

Information security teams should adjust to a higher order of thinking for long-term success and monitor behaviors and anomalies that differentiate from baseline healthy activity. For example, a user who downloads excessive amounts of files in non-peak hours might require further IT investigation. It's all about the combination of technology and human behaviors, not one or the other or one over the other.

TAG Cyber: What is the future of enterprise information management, and how do you see that impacting data security?

OPENTEXT: Thematically we see the market needs around enterprise cloud services and cloud access, collaboration, and secure information exchange as long-term trends that we will continue to develop around. The business benefits of the cloud are obvious—cost, efficiency, accessibility—but the cloud expands and compounds the attack surface that security teams are tasked with protecting. A focus on user behavior analytics will be a necessity to address these types of threats.

AN INTERVIEW WITH WITH IDO SAFRUTI, CO-FOUNDER AND CTO, PERIMETERX

MANAGING BOT-BASED ATTACKS WITH THREAT DETECTION

The term "digital transformation" has been in the popular business lexicon for quite a while. In the wake of the COVID-19 pandemic, we've seen changes to the digital world that no one could have predicted, including a significant and sudden uptick in online transactions and interactions—all at a startling pace. Satya Nadella of Microsoft wrote, "In this era of remote everything, we have seen two years' worth of digital transformation in two months."

As the world has become more digital, businesses must transform risk calculations, and one area that often gets overlooked is bot-based activity. Bot traffic mimics people, automatically testing username/password combinations and credit card information on websites. While credit card skimming used to be considered a physical threat from a point of sale, it can now happen anytime business is conducted online. Additionally, so-called shopping assistants offer coupons that distract shoppers from their path to purchase, sometimes redirecting shoppers to a competitor's site for a similar product or the same one at a lower price.

Organizations need to recognize these hidden threats as they transform. To reduce cyber risk, and to protect revenue, organizations are turning to application protection solutions such as those from PerimeterX. The company's flagship product, Bot Defender, is a behavior-based bot management solution which helps stop bot attacks and keep companies free from account takeover, carding, and operational disruption. We spoke with Ido Safruti, co-founder and CTO of PerimeterX, about why companies can't forget about web-facing threats.

TAG Cyber: Attackers' techniques are ever-changing. Are bots getting more sophisticated? How so?

PERIMETERX: Yes, bots have grown in sophistication over time, and attacks that used to happen only on the world's largest websites are now happening on smaller, popular websites such as those for food and grocery delivery.

Since the beginning of the COVID pandemic, we have seen an increase in "sophisticated" attacks using tactics such as headless browsers and JavaScript-enabled bots. Sightings of bots with detailed business logic capabilities to navigate multiple pages and ability to solve CAPTCHAs have increased, as have sophisticated account takeover (ATO) attacks against smaller targets. We have also seen an increase in botnets that are broadly distributed and have higher quality IP addresses—namely utilizing a large range of residential addresses.

It is likely that professional cybercrime rings responsible for sophisticated attacks are now broadening their targets to include more sites and smaller sites. It also appears that the tools to rent or create distributed botnets, as well as more sophisticated bot and ATO attacks, have gotten easier to use and become more widely available on the dark web.

The number of ATO attacks hasn't just risen proportionally—in some sectors we have seen a nearly 500% increase

TAG Cyber: What does that mean in terms of attack identification and mitigation?

PERIMETERX: Since attackers have shifted and found new techniques and more advanced tools, it will become hard to spot attacks early and will further reduce the efficacy of IP-address reputation as a way to spot bots. Now, it is more important than ever that businesses of all sizes use a sophisticated bot management tool that relies on behavioral analytics, advanced machine learning techniques, predictive models, and security research to block a wide range of sophisticated, automated attacks.

TAG Cyber: Bot Defender uses a combination of fingerprinting, behavioral analytics, and predictive models. How have you been able to extend its foundation to address more types of threats?

PERIMETERX: Because of the position Bot Defender plays in protecting the websites, web apps, and APIs of some of the largest e-commerce sites in the world, we are able to leverage the data and intelligence it gathers to address a variety of use cases.

Our Sensor collects and sends hundreds of client-side indicators and signals to the PerimeterX Detector. These signals are used to create baselines for validation of human versus bot activity, identification of suspicious script activity, and malicious browser extensions. The Detector maintains a repository of known attacks across all protected properties, so malicious actions can be blocked quickly. Our Enforcer is the gatekeeper for threat response policies; it enriches and mitigates automated traffic according to business needs. These components are used across our current portfolio to protect enterprises from automated attacks and client-side threats like digital skimming and Magecart, as well as from browser malware.

From day one, our approach was to use the same infrastructure to support multiple solutions, so we built the PerimeterX platform with extension in mind. It's gratifying to see that vision and planning come to fruition. In support of this, we recently introduced Code Defender and Page Defender, which leverage the company's Sensor-Detector-Enforcer approach to stop digital skimming and Magecart attacks and stop coupon assistants from disrupting your website visitors' paths to purchase.

TAG Cyber: There are a variety of attack methods used on websites and web applications, what are you seeing most in customer environments?

PERIMETERX: Attack methods have grown in frequency and sophistication over the last few years. While we've seen a variety of attack methods of late, two rise to the top: ATO and digital skimming, often known as Magecart. In an ATO attack, attackers

try to take credentials and control accounts to gain access to free content, personal information, credit card information, loyalty points, rewards, or other benefits. The number of ATO attacks hasn't just risen proportionally—in some sectors we have seen a nearly 500% increase since the shelter-in-place directive went into effect across the world, while legitimate traffic was up only 25%. We've also seen an uptick in Magecart attacks in which malicious code is injected into a website's code base to skim personal information such as email addresses, passwords, and credit card numbers from site visitors.

TAG Cyber: Why is the platform approach important in today's environment?

PERIMETERX: Leaders in digital businesses are looking to leverage the capabilities of a trusted vendor and to gain synergies by working with solutions that can address multiple challenges. Consolidation of point products onto a single cloud-native platform gives the team managing application security visibility into the broader threat landscape, a single dashboard for web analytics, as well as data that is correlated and enriched for more thorough analysis. This approach saves teams from manual correlation and helps them make accurate decisions quickly. Increased efficiency means that DevOps and SecOps teams can focus their efforts on value-added services and bringing new applications to market more quickly. Ultimately, it frees valuable technical resources to focus on growth.

AN INTERVIEW WITH WITH MIKE McKEE, EVP AND GM, INSIDER THREAT, PROOFPOINT

EMPOWERING SECURITY TEAMS TO REDUCE INSIDER THREAT

Insider threat has always been a complicated problem. At a certain level, companies have to trust employees to access and use the data and systems for which they are authorized. Compensating cyber security controls should always be implemented, but preventing risky behavior while affording the access employees need to do their jobs is nuanced. In a world where significant portions of the workforce are remote, using unmanaged devices, and where 24X7 access is a given, companies can struggle to determine inappropriate behavior before a compromise occurs.

Finding anomalous or malicious behavior requires a deep baseline understanding of data movement as well as context around users' actions. Identifying and analyzing the right intelligence—which is more than just reams of data—is key. ObserveIT, now a division of Proofpoint, is the leader in the insider threat space, helping customers find threat signals and respond to threats as they're happening. We spoke with Mike McKee, EVP and GM of Insider Threat Management at Proofpoint, to discuss the risk.

TAG Cyber: When companies refer to "insider threat," they often mean the threat of employees causing harm. Why does this not paint the whole picture?

PROOFPOINT: Our work world is pretty complex and nuanced today. For many businesses, work is not done just by employees, but also by third-party contractors, outsourcers, and managed service providers. In fact, one in five jobs in America was held by a non-employee worker as of 2018[1], and that number is only growing year over year. This means many users with access to protected data and infrastructure do not have the traditional employee-employer relationship.

Furthermore, we see digital transformation of supply chains resulting in customers and suppliers sharing data infrastructure. This also means extending access to sensitive IT resources to a broader range of users. This is why we've pushed to expand the definition of "insider" to include anyone who has authorized access—whether that's a traditional employee, a temp worker, a long-term contractor, a service provider, or a supply chain partner. Every business will have different types of insiders, with different levels of access and different risk profiles. There's not a one-size-fits-all definition of an insider, but "employee" alone does not properly describe the category.

[1] *https://www.npr.org/2018/01/22/578825135/rise-of-the-contract-workers-work-is-different-now*

TAG Cyber: There are different categories of risky insider behavior. Can you share what they are and how each one presents a different type of risk to the organization?

PROOFPOINT: We typically break it down into three main categories of risky insider behavior: accidental, malicious, and unknowing.

"Accidental" (a.k.a. careless or negligent) refers to insiders who are just trying to do their jobs, but who may be doing something that is outside the corporate security policy or otherwise risky. There are more examples of this than ever before with the rise of remote work. Doing work on an unsecured Wi-Fi network; forwarding sensitive work data to a personal email account; printing sensitive data; the list goes on. The common thread is that the person is not trying to put the business at risk but may be doing so by operating outside the bounds of security rules. This is far and away the biggest proportion of insider threats at 63% (Source: Ponemon 2020 Global Cost of Insider Threats Report). The average annualized cost to an organization for accidental insider threats is $4.58M. So, while it's not intentional, it's also not harmless.

Malicious (a.k.a. criminal) insiders are those who are misusing their access on purpose. They may be exfiltrating customer data or stealing corporate IP, but the common thread is their intentional abuse. This is the second most common type of threat, at 23%, and costs an average of $4.08M per year per organization.

Finally, we have the "unknowing" category, otherwise known as credential theft. This means someone's user ID and/or password were stolen, and someone impersonated the user to steal or misuse corporate assets. Credential theft represents 14% of all insider threats and costs organizations an average of $2.79M annually. As you can see, the different types of threats happen at different frequencies and costs to the organization. All are dangerous, but they are different in key ways and it's vital to be able to differentiate between them (based on intent and what really happened) in order to respond properly to an incident.

many users with access to protected data and infrastructure do not have the traditional employee-employer relationship.

TAG Cyber: It's not unheard of for an employee to feel like their privacy is being breached with insider threat solutions. How does ObserveIT manage to balance personal privacy and protection against inappropriate behavior?

PROOFPOINT: Balancing employee privacy with security is a challenge that every organization, every executive, every board member needs to grapple with. Different organizations must strike different balances based on applicable regulations, on their specific security concerns, and based on their company culture.

ObserveIT is highly customizable to fit our customers' specific privacy needs. Everything can be anonymized by default; we call it "privacy by design." Our customers have the ability to fine-tune exactly how they use our privacy settings, but we give them the power to anonymize users up until the point that it becomes clear actual wrongdoing has taken place

and HR, legal, or other serious action is required. We let our customers define activities that are off limits for monitoring—such as personal banking, medical insurance, or social media. We also build in a "watch the watchers" functionality to ensure that those with access cannot violate user's privacy. While security is of utmost importance to the modern business, privacy combined with regulations such as GDPR and CCPA are now both a norm and a law in many places. ObserveIT is purposefully designed to help businesses preserve the privacy of their users.

TAG Cyber: How do things like remote work and DevOps impact organizations' abilities to effectively monitor insiders?

PROOFPOINT: When it comes to remote work, modern IT has a big job on their hands increasing the resilience of their systems. DevOps presents a similar challenge, in that its tenets and workflows often give certain users a huge amount of control and power within critical systems. There are five main areas we recommend focusing on when it comes to security:

- One, train your users on security best practices and give them the tools they need to work from home securely (e.g., VPNs.)
- Two, limit access to what is needed, and ideally to the timeframe in which it is needed (you'll know this as least privilege access).
- Three, test your strategy and look for holes. For work from home, this means testing out your secure remote access strategy and ensuring it both meets the needs of your workforce and plugs up any security holes.
- Four, use multi-factor authentication as broadly as possible across the organization (this really helps with securing BYOD and decreases credential theft risks.)
- Five, aim for visibility. The more you can see what is happening across your critical systems and data, the better you can respond to threats as they arise.

TAG Cyber: What things should we be looking for from ObserveIT now that you are part of Proofpoint?

PROOFPOINT: We have a couple of exciting announcements coming up over the next few months and beyond. We're looking forward to becoming a deeply integrated part of the Proofpoint Information Protection platform and strategy. Proofpoint has proven to be an ideal partner for us, and there's a genuine and strong synergy between what we've been building with ObserveIT and Proofpoint's people-centric approach to security. We're looking forward to offering our joint customers a unified suite of security products that helps them avoid dealing with disparate solutions that often don't play nicely together. We think it's a great example of the whole being more than the sum of its parts.

AN INTERVIEW WITH WITH DAVID WOLPOFF, CO-FOUNDER & CTO, RANDORI

BUILD SECURITY PROGRAMS RESILIENT TO RISK, NOT THE LATEST VULNERABILITY

Testing your security defenses is foundational. Without an understanding of your weaknesses, it is nearly impossible for the security team to accurately and efficiently decrease risk. Traditionally, organizations have relied on a combination of testing methods including vulnerability scanning and penetration testing. Vulnerability scanning is the least intrusive way for organizations to assess weaknesses in assets. However, scanners rely on a database of known vulnerabilities and thus can't handle zero days or advanced attacks. Penetration tests go deeper; testers use a combination of scanning and manual techniques to find vulnerabilities, and then attempt to exploit them to determine the organization's risk. That said, penetrations tests are generally designed to assess a limited portion of the organization's assets.

Red teaming is by far the most thorough type of security testing, as it is designed to simulate a real-life attacker's tactics and techniques. But quality red team assessments require dedicated resources and a big budget.

Former Carbon Black VP Brian Hazzard and red teamer David "Moose" Wolpoff founded Randori to build an automated red team platform accessible by any size organization. We spoke with David Wolpoff, Co-Founder and CTO, about this area that's quickly gaining traction among enterprises.

TAG Cyber: First, can you explain what a red team assessment is? I think there's a lot of confusion with pen tests.

RANDORI: As a former enterprise red teamer, people regularly ask me, "Should I do a pen test or hire a red team?" The answer comes down to the question you want to answer.

A pen test will tell you if a specific set of security controls are working as designed to work but will not provide insight into your security program's overall effectiveness. A red team assessment focuses first and foremost on delivering an authentic evaluation of your ability to adequately defend against an adversary—real attacks, real targets, real objectives. It's the closest thing a security team will get to a live-fire exercise.

Questions a pen test will answer:

- What public exploits am I vulnerable to?
- Does this security control work as expected?
- Am I getting the right alerts?

Questions a red team engagement answers:

- How hard is it for an adversary to breach my organization?
- Is my security program working as expected?
- When unexpected things happen, can my team respond under pressure?

TAG Cyber: What are some of the secrets you learned as a red teamer that you built into the platform?

RANDORI: We founded Randori to be able to provide organizations an internal red team capability. That means the experience needs

Rather than fixating on the specific issue, we encourage our customers to focus on enacting changes

to be authentic, dynamic, and provide CISOs the necessary confidence and information to build board-level trust.

Like any real adversary, the product starts with recon. The Randori Recon engine is "Black Box" —meaning we start with very little information, like an email, to kick-off our continuous reconnaissance—just like a hacker would determine what's connected to an organization.

From there, we flavor that information with what we call "Target Temptation" to identify what things to attack first. Just like a real attacker, Randori is always working against an objective. Security teams looking at a list of top targets on the Randori platform can use Randori to determine why that target is tempting, and through the use of attack, understand if there is a route to the company's "crowned jewels," i.e., most valuable commodities.

Unlike BAS (breach and attack simulation) solutions, the Randori attack experience is both safe and authentic. When a user launches a Randori attack, they will be learning how to protect their unique environment and a deeper understanding of how to protect their real production assets. Hence the meaning behind the company name Randori, which means "freestyle practice against an adversary."

TAG Cyber: Before a company conducts a pen test, red team assessment, or deploys a platform like Randori, how should they prepare?

RANDORI: First, start with the basics. The point of a red team engagement or a penetration test is to learn. If there are things you already know you need to address, address those first. After that, you should stress the entirety of a program to see how hard it would be for an attacker to zig-zag through an organization.

Secondly, not every security program is ready for a red team engagement. Don't jump to bringing on a high-end red team unless you're prepared for high-end learnings. If you're still focused on blocking and tackling, maybe you're not ready to get a red team to beat you up.

TAG Cyber: No type of security testing is beneficial unless something can be done with the results. How does Randori help with remediation?

RANDORI: It's an interesting question and one that comes up with almost every customer. I'll give you the same answer that I used to give on red team engagements, and I now use talking with Randori customers.

The goal of Randori is to challenge your assumptions. We leverage our perspective as an adversary to raise questions,

uncover issues, and identify process failures organizations may otherwise overlook. We are not trying to find every vulnerability; instead, we aim to help organizations up level their security program by identifying systemic failures and empowering their teams with the skills needed to get to the root cause. Sometimes that's a patch—but far more often remediation in the Randori context involves providing security teams with the evidence they need to change processes and training. Rather than fixating on the specific issue, we encourage our customers to focus on enacting changes, such as network segmentation, improved visibility, and better training. These things allow companies to build security programs resilient to entire categories of risks, not just the latest vulnerability.

AN INTERVIEW WITH WITH KURT VAN ETTEN, CHIEF PRODUCT OFFICER, REDSEAL

DIGITAL RESILIENCE IN A WORLD OF IoT

The network sees everything: the number and type of devices touching the network, the amount of data flowing through it, communication paths between entities, access requests, and more. Whether the network is on-premises, cloud-based, multi-cloud, or hybrid, for organizations to manage and protect what is on their networks—regardless of location—they need clear insight into network activity, ideally in a holistic, unified way.

In many cases, though, gaining that holistic picture of the network, understanding risk, and ensuring digital resilience are problematic. The ephemerality and complexity of today's networks make it hard for organizations to see what's on their networks, add context, and calculate risk, and then apply policies which demonstrably decrease risk. RedSeal provides an automated analytics platform that allows companies to achieve the insight mentioned above, and we recently spoke with Kurt Van Etten, Chief Product Officer, about building digitally resilient organizations.

TAG Cyber: So many vendors in our space focus on a security-first message, but RedSeal's anthem is digital resilience. Why, and what are the subtle differences between digital resilience and providing security that allows companies to operate optimally?

REDSEAL: Digital resilience is a strategy that encompasses prevention but also includes being prepared to respond to and recover from an incident. To do this, organizations need a deep understanding of what they have, how it is connected, and what is at risk. With this foundation, customers can build the proper policies and procedures not only to prevent attacks, but also to quickly respond and recover from attacks.

TAG Cyber: We've worked together on healthcare-specific research. Why is this area important to RedSeal and what are some of the unique security challenges in healthcare?

REDSEAL: Healthcare security teams have a tremendous challenge—protecting valuable data in a dynamic environment. While all security teams have to be careful not to impact network performance or availability, in healthcare, availability can literally mean life or death. Let's take patch management, for instance; in a non-critical industry, deploying patches is hard enough. In healthcare, add in the requirement to keep systems up and running 24X7; no downtime is acceptable, but yet an unaddressed vulnerability in a healthcare system could lead to exploit, which could have devastating, life-threatening effects.

The healthcare industry is also experiencing a dramatic increase in connected devices. From tablets used to record and track patient data to wireless heart rate monitors and connected heart pump valves—the Internet of Medical Things is

Once these devices are identified, customers are able to move them from "unmanaged" to "managed" and to update their systems of record.

exploding. Security practitioners are constantly challenged to discover, locate, and secure medical IoT devices, many of which were not build with security in mind. Connected IoT devices make health data more accessible and help manufacturers monitor the state and status of devices, but it also introduces a risk not seen before in these kinds of devices. Keeping those often un-patchable IoT devices protected behind firewalls and with strict access controls is critical.

The healthcare industry is also going through the same digital transformation as other industries as they adopt both SaaS and IaaS solutions. Now, healthcare security practitioners need to consider the implications of where data is processed and stored, who has access to the cloud, how access is controlled, and how compliance mandates are met in a cloud environment.

TAG Cyber: RedSeal works by creating a model of the network environment; why is this the first step and what data are used to do so?

REDSEAL: RedSeal begins by helping customers understand their networks. We collect configuration data from IaaS, software-defined networks, cloud, and on-premises solutions. Then, we calculate the access paths between each device, virtual or not. There are two main results. First, we discover network devices a customer doesn't know about. Once these devices are identified, customers are able to move them from "unmanaged" to "managed" and to update their systems of record. Then, we find gaps in customers' knowledge of their endpoint systems. To identify these inventory gaps, RedSeal customers upload endpoint data from all their sources and compare the differences. We find gaps in vulnerability scan coverage, patching systems, and endpoint agent coverage.

TAG Cyber: Why do you think healthcare continues to be a target of cyber attacks?

REDSEAL: Healthcare data is extremely value data for attackers because it includes personally identifiable information (PII) beyond email addresses and passwords. It can include credit card information, insurance information, billing addresses, birthdates, diagnostics, prescription information, family histories, and more—all of which can be used to compromise people's identities. In addition, and as a result of the personal specificity, healthcare data commands a high price on the black market so it's also attractive to cyber criminals seeking financial gain. Furthermore, the digital resiliency challenges mentioned earlier—the requirement for 100% uptime and availability and the problems with systematically addressing vulnerabilities—means cyber criminals can target healthcare organizations when they know there is likely to be a vulnerability. They become an easier target of opportunity.

AN INTERVIEW WITH WITH ANDY PROW, CEO & CO-FOUNDER, REDSHIELD

REMEDIATING VULNERABILITIES AT SCALE

Since the advent of the first firewall, cyber security controls have revolved around the use of barriers or gateways to prevent bad from entering "safe spaces," as it were. The idea of the barrier or gateway is solid, but security practitioners and vendors alike have seen over time how these technologies have had to dramatically adapt as the entities that communicate—and how they communicate—on networks have evolved. Today, applications are arguably the most important entity to keep up and running on an organization's networks: these are the business-critical apps that allow the company to generate revenue, serve customers, and keep employees happy. This is why it is critical that they also remain protected.

As such, application security has evolved from a domain in which the focus on writing hardened code has expanded to include attention to the controls that shield apps from unauthorized use, modification, and other exploits. Web application firewalls (WAFs) have become the main category for such protection, supported by API protection. RedShield, an eight-year old security company founded out of New Zealand, has modified and supercharged the concept of the Cloud WAF. Andy Prow, CEO and Co-founder of RedShield, spoke with us recently about the company's unique approach.

TAG Cyber: Application vulnerabilities are becoming hard for businesses to resolve. What are the more common complaints you hear about application security from your customers?

REDSHIELD: Most published breaches are caused by the exploit of vulnerabilities organizations are already aware of. This is primarily due the real-world constraints organizations face. For organizations with dedicated development, patching, and SecOps teams executing mature processes, rapid remediation of threats against applications is realistic. (Note that the average time from vulnerability disclosure to proof of concept exploit is 2 weeks, source: Kenna Security). However, a typical organization may have 5% of their applications in this state. For the other 95%, meeting these timelines is impractical.

Development teams' priorities, limited access to or experience with source code, patching dependencies, compliance restrictions, and tight budgets are reasons that discovered security code defects remain in development backlog and risk registers for too long. Then on the SecOps side, cleaning malicious traffic is an endless job. New issues are published every day and require continual tuning and deployment. Nonetheless, blocking masks should not block legitimate transactions; change management and testing is a nightmare. In reality, risk acceptance becomes the norm.

By deploying custom code objects (shields) that RedShield's developers write and maintain on the FaaS (function-as-a-service) architecture we operate, RedShield fixes vulnerabilities that are usually reserved for software developers, without touching a single line of application code. It's no problem for us to fix legacy applications, third-party apps, API's—all sorts, and we do this at speed.

One of the more current challenges organizations are faced with is balancing the need to maintain security while more aggressively focusing on digital transformation efforts—likely with resource constraints. To do this effectively, organizations need to enable security and development resources to focus their time on digital transformation and innovation efforts and limit the time they're distracted by patching application vulnerabilities.

Shielding vulnerabilities helps in this regard as it removes vulnerability risk straight away and gives organizations time to decide when they might remediate the application itself. And it means development and security resources' time isn't constantly distracted so they can focus on more commercially productive tasks.

TAG Cyber: WAFs don't typically include vulnerability remediation, but the first step in RedShield's process is guided remediation. Can you explain exactly what this entails?

REDSHIELD: When supplied with a list of security defects, RedShield provides a Shielding Plan that highlights how our developers would fit each problem with the code objects that we would either get from our library or custom develop. We send the customer development team our recommendations, and they can choose to take that advice and develop the fixes themselves or have our team deploy the software object shields.

A WAF examines traffic—it has nothing to do with the functioning of an application; fundamentally it looks to protect rather than to fix. There is a small area of overlap where application-specific tuning may appear to address reported exploitable flaws, however this overlap is much smaller than many vendors state. We, too, include WAFs as part of our solution, but we take operational responsibility for tuning both for compatibility and effectiveness whilst adhering to customer change management. We use purchased and built AI tools to assist in decision making, then automation and orchestration to ensure accurate and complete process execution. We can also provide skilled engineers and analysts to resource-strapped companies, providing our customers mature processes 24x7.

Our approach is in line with risk treatment practices developed during the industrial revolution for health and safety: Eliminate, control impact, restrict access. In our world, it looks like this:

ELIMINATE: REMEDIATE VULNERABILITIES RIGHT AWAY (USING SHIELDS – CODE OBJECTS)

We're able to deploy a code object shield for applications, often in a matter of minutes rather than the weeks, months, or even multi-year timelines typical with software remediation. This is because, over the years, we have written thousands of code objects (shields) that fix all kinds of vulnerabilities. This shield library means we can, in the majority of instances, immediately remediate

Instead of just filtering like a WAF, shields actually fix the issue by changing the application behavior

vulnerabilities on companies' risk registers without touching the application's code. And for any unique shields that might be required, our team can write those specific shields right away (and then add those shields to our customer community shield library).

CONTROL IMPACT: ADD FURTHER PROTECTIONS

We then provide a further suite of protection to reduce remaining threat surface without impacting experience. We detect and block the constantly-evolving barrage of malicious traffic without blocking customer transactions, and also test our remediation to ensure that the effectiveness of the solution and functionality is retained weekly.

RESTRICT ACCESS: HUNT ATTACKERS

We use both community intelligence and observed behavior to identify malicious bots or human actors. We simply stop them from being able to perform any action on web apps.

TAG Cyber: What not just block or quarantine bad apps?

REDSHIELD: That is certainly an option: turn off apps with known vulnerabilities, quarantine them, block them, etc. However, depending on the application, it has a bearing on the validity of such an approach. What if the app has business importance; can you afford to take it offline or limit usage? What if your web app is critical for taking orders and you take it offline?

For instance, a European commodities trader approached us with a trading portal which was found to have issues. Due to GDPR concerns, their legal department demanded it be taken offline immediately. As a result, the company had to revert to email, phone, and fax to convert trades. The developers stated that fixes were possible within a 6-18 month timeframe—because it is a financial trading platform, there are technical, audit, and compliance hurdles to launching a new portal. However, even at six months, that is a long time for the traders to not have a working platform. Instead, RedShield was able to fix their platform and make it fully compliant in 48 hours.

Another example we had was with a large payment provider that offers credit card and EFT-POS payments. Their software had 300+ issues; not fixing them would have resulted in either a breach (with some probability) or failed compliance. In turn, this would mean that banks would not have allowed the provider to hold client credit card details and their value as a business would have been reduced. It took six weeks for RedShield to fix all of these issues—and biggest lag was sharing information about the details of the finding.

In our opinion, it's better to shield or remediate problems rather than just blocking communication from happening. Instead, if you fix the problem, you reduce the threat surface. Using shields, we perform functions to remediate vulnerabilities—without the client

needing to involve developers, without touching application code, and we do this at speed and scale.

At RedShield we've also mapped our process and tooling to the framework developed by the National Institute for Occupational Safety and Health in the United States—the NIOSH risk reduction hierarchy. They know a thing or two about managing and optimizing risk, they have 150 years of experience!

To illustrate the point around blocking bad apps, let's take at a metaphorical example of a hazardous liquid spill. Now, you could cordon off the area to make sure workers don't go near the spill. You could produce warning signs and place them in front of the area as a warning. Or you could provide better safety boots—which would be most akin to deploying a WAF on a network. While these are certainly good steps, and they improve the immediate safety of workers, they should be done only as part of the larger hygiene sequence.

RedShield cleans up the spill, puts in new flooring to prevent future spills, updates workplace protocols, and then also provides the newer boots. You're not only better protected than before, but you're better protected in a safer environment.

TAG Cyber: How is a shield different from a next-gen firewall?

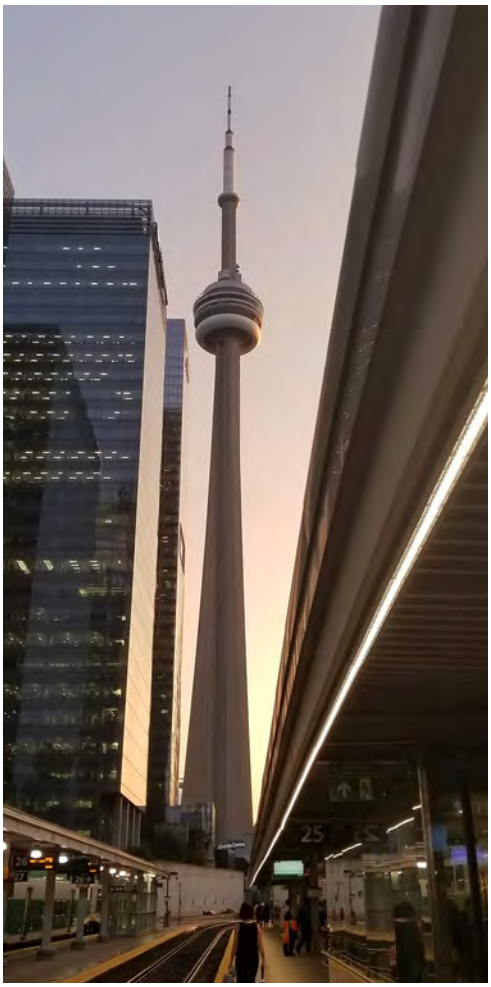
REDSHIELD: A next-gen firewall examines network traffic and filters traffic based on signatures or heuristics, often using IPS or signature matching technology.

The first problem with IPS technology is that through encoding, padding, splitting, or encryption the payloads can be easily obfuscated and hence slide past the inspection engine. To address this, fifteen years ago the industry introduced a web application firewall (WAF), primarily designed to achieve the same outcome. WAFs typically include an internal web server, which means that the full application request is first decrypted and aggregated before the analysis step is performed. However, like IPSs, WAFs have become security tools that disrupt legitimate transactions and absorb limited resources to maintain. Their chief problems are:

1. They don't secure any insecure application transactions, causing failed audits and missed launch dates—dev teams still have to fix these;

2. The controls a WAF uses, limiting what a user is allowed to do, are able to be bypassed, and these controls unavoidably lead to false positives.

This second limitation led to the genesis of NG-WAFs, where the focus is to detect and block bots; real-time threat protection is no longer the goal.



NGFWs or NG-WAFs can't resolve exploitable elements within an application, they only see as far as the rule set with which they've been programmed to filter traffic. The task of resolving underpinning code or logic issues remains the responsibility of developers, and without these fixes, audits are failed, project deadlines not met, and fundamental legacy systems are forced from production.

A shield is a block of code that modifies application behavior to fix a known exploitable vulnerability. They are nano-services that become a functional part of the application. For the exploitable flaw to be secured, all traffic must flow through the shield, hence traffic is forced through a reverse proxy hosting the shield, placed in front of the application. By ostensibly eliminating the vulnerability and thus reducing the threat surface that an attacker can exploit, the issue is resolved without the need of a development team to engage in software remediation.

A shield is an in-path solution where all HTTP traffic for the application travels through RedShield where additional protections are added before passing through to end users. Shielding doesn't limit what a user can do, but rather changes the application transparently so that anything malicious has no effect and doesn't disrupt the user experience. Instead of just filtering like a WAF, shields actually fix the issue by changing the application behavior, without changing the underlying code itself. The flawed application is rendered safe while retaining its functionality—attacks are stopped, but transactions aren't.

So while a WAF promises to protect through increasingly complicated policies, shields address the root of the problem. For example, if your app accepts weak passwords, WAF policies might be deployed to check geolocation, frequency of attempts, the method of access, time of day, or countless other data points. The problem is, as compatibility issues inevitably come to light and the challenge of constant updates and maintenance becomes apparent, most businesses make their controls less and less effective to maintain app functionality. A shield implements better behavior for the application.

TAG Cyber: You ran a pen testing company for ten years; what inspired the transition to building a security product?

REDSHIELD: After starting and building NZ's largest pen testing company, I found that when we visited our clients to check in and re-test their applications, we found the same vulnerabilities again. Clients often found it too difficult to clean up their risk register for various reasons and were left in a situation where their security posture kept getting worse. After a while this became frustrating. RedShield was born out of this experience. Remediating all vulnerabilities found from a human pen test quickly and at scale is an area no one else is really addressing and we wanted to take on this challenge.

AN INTERVIEW WITH WITH MIKE ARMISTEAD, CEO, RESPOND SOFTWARE

AUTOMATED DECISION MAKING FOR THE SOC

Enterprise security teams have no dearth of tools to identify, map, correlate, monitor, and report data from their technology ecosystems. Whatever the environment—cloud, on-prem, hybrid—there are tools to produce data: traffic data, access data, endpoint data, anomaly data, and more. In fact, security operations teams are grappling with so much data that it can be hard to find the signal amongst the noise, especially when teams are shorthanded and overworked.

As such, automation has become a SOC analyst's best friend, yet, the question always remains: Is this the right data? Analysts need confidence that the data they're receiving is real-time, accurate, and actionable, and that false positives are kept to a minimum, allowing them to focus on the higher-level operations tasks which will have a maximum impact in protecting the organization from compromise.

Mike Armistead, CEO from Respond Software, spoke with us about the company's Respond Analyst and how SOC teams are using it to accelerate incident triage and response.

TAG Cyber: Can you please explain how the Respond Analyst differs from a SIEM and a SOAR?

RESPOND: SIEM is a collection of rules. SOAR is a collection of playbooks. The Respond Analyst is an automated decision-making solution.

SIEMs are focused on the logs they manage—this creates a set of alarms based on whatever the SIEM provides. There is no analysis or decision making. It's a classic security data lake. The SIEM uses rules written by the security team to filter the number of alerts to a much smaller number, typically 100:1 or even 10,000:1. Their tuning demands a significant investment of time and attention, and by nature excludes potentially useful and valuable information—the true signals of an attack can be ignored, overlooked, or missed. SIEM is a collection of rules, which leaves room for error and inconsistency. Implementation of SIEM is just one step on the journey to security automation.

SOAR tools require a great deal of programming in order to translate their theoretical promise into real-world operational efficiencies. For many security teams, this is a resource-intensive process that demands many hours of labor to build playbooks and develop custom integrations. That's why SOAR solutions are best suited for use in mature security operations programs; these organizations have the largest number of skilled employees, and (ideally) the most time to spend on complex engineering tasks.

While SOAR tools are capable of automating parts of the incident response component of the security incident workflow, the Respond Analyst fully automates the discovery portion of that workflow. The Respond Analyst arrives prepared to handle millions of events per day and is already

Good security requires curiosity as to what's going on beyond what the machines are saying.

capable of escalating only those that are truly worthy of human attention. The Respond Analyst is as close to "plug and play" as possible in a SOC, in that it is able to reason through all the alert data that's collected in the environment on its own. There are no rules or playbooks, and there's nothing to configure. Out of the box, the Respond Analyst is ready to detect and escalate only those incidents that are malicious and actionable. The difference is that we've moved from basic workflow automation to reasoning and decision automation. The Respond Analyst understands the products, alerts, and enrichment sources in your environment and knows when and how to put the puzzle together.

TAG Cyber: How would you answer the question, "Isn't this just another alerting tool my analysts have to manage"?

RESPOND: I'd say it's the exact opposite! We investigate and make decisions on every alert, so the analyst doesn't have to. The Respond Analyst will determine if an alert indicates a true threat or is just another false positive by considering three different areas of context:

1. Internal Context: This includes the system's business function, importance, location, and vulnerability—and evaluates the data's significance. Context about internal systems helps the Respond Analyst understand if the observed attack is relevant to the targeted system, and it helps prioritize the incident.

2. External Context: Since only an IP address is included in the event, an external context can show who owns the IP address and its geolocation. The Respond Analyst can understand more about the attacker, the attacker's intent, and if other organizations have been targeted.

3. Historical Behavior Analysis: By spotting historical patterns of the behavior and associations of systems and accounts, the Respond Analyst can determine whether the observed activity is malicious or normal behavior. Incidents unfold over time and involve multiple data sources. The Respond Analyst can determine if the data source is external or hidden within authorized system administration tools.

TAG Cyber: On your website and in your collateral, you emphasize human judgment as an important element of event handling and incident response, but the technology is heavily focused on automation. How do you achieve a good balance between saving people time yet needing them to quickly find the right data?

Respond: Technology makes analysts more productive. It's an efficiency tool to eliminate the repetitive and mundane tasks. Technology platforms collect the data for automation, normalize it, and put it where someone can do something with it. That last step has traditionally been driven by humans. Our goal is to

automate those human decisions—what we do based on the information and how we do it.

Machines offer consistency, infinite scalability, and the ability to handle millions of instructions per second to solve complicated problems using huge amounts of data that no human could ever match. However, SecOps automation needs the collaboration, curiosity, and creativity that only people can bring to the table.

Automation requires that people work with machines, too. You tell a machine what you believe, and it can tell you if you're right. Good security requires curiosity as to what's going on beyond what the machines are saying. As they autonomously monitor, people can watch for the novel and the exceptional; that requires creative thinking. SecOps automation not only requires collaboration between people but also with their tools. Even though automation is about reducing the need for people, automating SecOps still requires creative, curious people in the SOC to collaborate with stakeholders across the organization.

TAG Cyber: Many large enterprises are using industry frameworks to shore up security operations. What is your take on this approach?

RESPOND: The MITRE ATT&CK framework is one approach that has been widely discussed—and given much praise—in the cyber security industry. We agree. It meets a very real need: it provides a list of methods by which enterprise IT environments can be compromised, and the information is detailed and highly specific.

Any of the attack scenarios described in the ATT&CK framework can be emulated by red teams or during penetration tests. And, because it's behavior-focused, the framework can help security teams understand the "how" and "why" of particular malicious activities. Security teams can employ the ATT&CK framework as a way to map their sensor grid's detection capabilities against real-world attackers' tactics, techniques, and procedures.

If you can defend against every technique that's mentioned in the framework, the common wisdom goes, your environment will be fundamentally secure. But the framework is large and complex—it includes more than 500 adversarial techniques. It would be extremely challenging—if not downright impossible—for any organization to defend against all of them, all the time, completely.

Given the MITRE ATT&CK framework's complexity, it's nearly impossible for security analysts to achieve real coverage of even a small fraction of the attack methods it catalogues. This is another example of how decision automation software can power security operations teams to perform at an entirely new level.

AN INTERVIEW WITH WITH PAUL TRULOVE, CHIEF PRODUCT OFFICER, SAILPOINT

KEEP TRACK OF USERS—HUMAN AND NON-HUMAN—WITH ADVANCED IDENTITY GOVERNANCE

As identity has become the so-called "new perimeter," enterprises need faster, easier, and more reliable ways of governing identity across users, systems, and networks. Furthermore, the definition of identity must now include machine identities and process identities, in addition to user and device identities. But it's not just about managing identities today; identity has become a quasi-control plane upon which security decisions are made: Should this person have that access to that resources? Can this device touch these files? Is this machine-to-machine communication permitted, and is there anything suspicious about what's happening right now vs. last week?

These are all questions that can be answered with proper identity governance. And SailPoint is leading the space with their automated and orchestrated platform predicated on SailPoint Predictive Identity™.

We spoke with SailPoint's Chief Product Officer, Paul Trulove, to learn more about what the company is doing and how they're helping companies manage multi-cloud infrastructure and the systems, apps, and data that communication on them.

TAG Cyber: SailPoint has a lot of tenure in the market. Tell us a little about the genesis of the company and product?

SAILPOINT: SailPoint was one of the first identity governance companies when we got started back in 2005. Our founders and early team members drove the definition of the identity governance space by focusing on gaps that existed in legacy provisioning products, which completely lacked security and compliance features. A few years ago, and still today, companies became inundated with a wide range of regulatory requirements and compliance frameworks—SOX, PCI DSS, COBIT, COSO, and NIST, to name a few—and that dominated the conversation.

SailPoint focused on building a solution to streamline how large, complex enterprises governed access to critical financial systems and other high-risk applications. In the early days, we focused on access certifications, separate-of-duty policy administration, and role management. As time went on, SailPoint built both a deep understanding of who has access to what and who should have what. So, in early 2010, we launched the next logical step of the puzzle with our plan to go into the provisioning space. This allowed us to help organizations see who has access and then provide them the tools to provision the right access to the right person at the right time.

Since then, we've continued to be the innovators in identity, pushing the boundaries in identity

Whatever identity management system you choose, make sure it can connect to where the applications are running

governance both in terms of scope and the actual definition of the market. For example, we firmly believe that identity governance must have oversight into human and non-human entities and their access. We also believe identity governance must govern users' access to applications and systems and the sensitive data that often lives in file storage systems today. And, with our latest vision, SailPoint Predictive Identity, we are again defining the future of identity through the lens of artificial intelligence. These are just a few examples of how we've evolved continuously the way identity governance is done to match our customers' dynamic business needs' speed and velocity.

TAG Cyber: What are some of the more salient threats you see affecting the identity space?

SAILPOINT: Early identity management deployments tended to focus on a small number of sensitive or high-churn applications. With the rapid evolution of enterprise IT environments due to digital transformation, there's been an explosion in the number of applications and the amount of data stored outside of a traditional database. Many organizations have struggled to keep up with the pace of change. As a result, many of their critical business and file storage systems are un-governed regarding identity and access management. This creates huge security and compliance gaps. We've recently seen this expand to include IaaS environments such as AWS, Azure, and GCP.

TAG Cyber: Legacy systems can present tremendous challenges for enterprises; how are most companies coping with that today, and where are the deficiencies?

SAILPOINT: Ultimately, all systems need to be managed and governed by identity management. To do that well, you have to address your legacy systems by building a comprehensive identity program. What you don't want to do is segment your legacy systems and silo them. If that happens, you miss the benefits of complete visibility and governance across all access. In terms of security and compliance controls, you have to have a comprehensive view. Don't allow yourself to be segmented in your approach to those things. Whatever identity management system you choose, make sure it can connect to where the applications are running, whether in the data center or the cloud.

TAG Cyber: SailPoint is an overlay rather than a replacement for other identity providers. What's the advantage?

SAILPOINT: Identity governance is a foundational component for any enterprise's security efforts. Historically, a common misnomer is that many companies will never entirely need identity governance if they have "good enough" access management in place. But access management is no replacement for identity governance. Identity governance and access management are

not an either/or scenario. Access management is essentially the "badge reader" of identity, granting access to the proverbial building. But access is just the beginning. Without the security and intelligence that identity governance provides, access management can become a source of business exposure if done in a silo without the identity governance brains backing it up.

TAG Cyber: How does identity governance facilitate digital transformation?

SAILPOINT: The thought is pretty simple: the digital transformation is all about moving processes and data online. The more you do that, the more access you create in the enterprise that has to be managed. Another critical aspect of digital transformation that is often overlooked is related to "external users" – customers, partners, vendors, etc. who are outside of the company and have access to systems and data for which access must be governed. By not including external identities in an organization's identity governance program, you can be overlooking one of the most common attack vectors in the enterprise.

And that brings us to non-human identities like RPAs and true robotics. These "AI" identities need access to critical systems, just like their human counterparts. Therefore, they need to be governed just like their human counterparts. Identity governance is the most foundational thing you have to do to drive digital transformation. In theory, an enterprise embarking on their digital transformation will become a sprawling landscape of identities, applications, systems, and data. This is where identity governance comes into play. Identity governance keeps track of users (human and non-human), centralizing everyone with complete oversight into who has access and whether they should have access.

AN INTERVIEW WITH WITH
ALEKSANDR YAMPOLSKIY, CEO AND FOUNDER,
SECURITYSCORECARD

RATING AND MANAGING ENTERPRISE SECURITY POSTURE

Enterprise risk involves more factors and components than most security teams can ever hope to track effectively. This is even more troubling with third parties and suppliers, where visibility into relevant security risk factors is less evident. As such, enterprise security teams have had to identify practical solutions to include the optimal categories of risk into an aggregate assessment of security posture.

In most cases, the development of a security rating has emerged as the best means for accomplishing this goal—especially for third parties. The use of a score allows for both absolute analysis of risk in quantitative form, as well as relative comparison of risk between peers. Modern tools accomplish this scoring by combining information collected from various means, including live collection of telemetry.

We recently had the opportunity to sit down with Aleksandr Yampolskiy from SecurityScorecard to learn more about how his company leads the industry in this important area of security risk scoring. We wanted to learn about techniques and trends in cyber security scoring, with emphasis on the practical requirements being requested by enterprise teams.

TAG Cyber: What specifically is it that SecurityScorecard delivers for enterprise customers?

SECURITYSCORECARD: SecurityScorecard helps enterprises manage digital threats with a 360-degree view of cyber security posture. Specifically, our security ratings solution provides visibility into the cyber security health of any organization from an outside-in perspective with an easy-to-understand A-F letter grade that is universally understood. This allows any organization to identify risk within their environment or any third party. Additionally, our issue-level details empower users to take action and remediate their cyber security threats.

With Atlas (our cyber security questionnaire and validation platform), enterprises can leverage our machine learning capabilities to automate the cyber security questionnaire exchange process for senders and receivers, making this cumbersome process two times faster. SecurityScorecard instantly maps cyber security ratings data to individual questionnaire responses, providing auto-validation of responses for a true 360-degree view of cyber security.

In addition to our Ratings and Atlas products, we offer professional services directly and through our channel partners. We continually work with our clients to align their most valuable assets—the technical knowledge, expertise, and experience of their employees—with overall organizational strategy and investment in third-party risk.

TAG Cyber: I know your algorithms are proprietary, but can you give us a feel for the specific factors you include in the development of a score for a given organization?

SECURITYSCORECARD: There are three main factors to think about during the development of a rating: data collection, attribution, and scoring methodology.

At a high-level, SecurityScorecard non-intrusively collects data from publicly available feeds across the internet by monitoring hundreds of different cyber security signals from a global network of sensors. Additionally, we operate one of the world's largest networks of sinkholes and honeypots to capture malware signals and further enrich our data set by leveraging commercial and open source intelligence databases.

Each issue we find is associated with one of our ten risk factor groups and is assigned a weight reflecting its threat severity. Some of our risk factor groups include network security, patching cadence, application security, and endpoint security. At scale, SecurityScorecard then attributes domains and IPs to organizations using automated processes, incorporating machine learning algorithms to optimize accuracy.

In terms of our scoring methodology, we calculate a rating based on an organization's digital footprint and observed security findings. To eliminate scoring bias, SecurityScorecard compares a company's findings to organizations of similar sized digital footprints. We make every effort to create and maintain cyber security ratings that are meaningful, accurate, and relevant. Our scoring practices allow us to continuously keep up with the emergence of new threats.

TAG Cyber: What are the trends in third-party risk assessment? Everyone knows that questionnaires have their weaknesses, so how do you get around this challenge?

SECURITYSCORECARD: What we've seen over the past couple of months, particularly as organizations quickly onboarded new technology partners to support remote work, is an increase in third-party risk. Third-party relationships and third-party risk management have been around for a long time, but the relationships between companies and their vendors, suppliers, partners, etc. has changed. Companies are dealing with even more third parties, increasing potential risk.

In today's environment, organizations are looking to automate their risk assessments

The change in landscape requires a second look at risk evaluation, especially as organizations are now focusing on business continuity and operating in a new normal. In today's environment, organizations are looking to automate their risk assessments and find a way to more efficiently virtually assess their third parties.

Assessments are one way of mitigating third-party risk, but we all know they provide a point-in-time snapshot, are time

consuming on both ends, and rely on vendor-provided responses and evidence, which often aren't satisfactory. With solutions like SecurityScorecard, organizations can continuously monitor their third parties, better prioritize when and how they assess their third parties, and validate vendor-provided responses with security ratings data quicker and with less effort.

Because on-site assessments haven't been possible this year, here are some ways security ratings and virtual assessments help address the current constraints. For example, if a third party's security assessment was positive last year and there have been no major changes in their relationships, technology, or security incidents, those are good signs. If they also have a positive and stable security rating, you can consider deferring their cyber risk assessment for six months to a year. Similarly, if a vendor's previous assessment was mixed, they've experienced changes, and they have a negative and declining security rating, that's a sign that this vendor should be prioritized and it's time for a full virtual cyber risk assessment.

TAG Cyber: Do you see any standard emerging in the area of security measurement and metrics? Enterprise teams would benefit, it would seem, from some commonality in this area. What's been your experience?

SECURITYSCORECARD: I agree, enterprises would benefit from some commonality, and we're noticing that cyber security ratings are emerging as a standard in terms of security measurement and metrics.

Reputable research firms have stated that cyber security ratings will become vital tools and a standard when communicating about cyber security risk.

Additionally, NIST SP 800-137 for Federal Information Systems and Organizations, recently added a continuous monitoring process. SecurityScorecard can help address this ongoing security monitoring and assessment need with Ratings and Atlas.

Security ratings provide organizations with an objective third-party security measurement, which is needed as organizations are working and sharing sensitive data with an increasing number of third parties. We're seeing SecurityScorecard become a requirement for a growing number of business relationships as part of best-in-class due diligence practices for providers and procurers of services.

We're seeing our ratings and reports used when IT and security teams present to their board or executives, so we expect this to become even more prevalent. My favorite quote around this topic is hearing from one of our customers that, "I used to

spend hours creating reports for board presentations. Now, with SecurityScorecard it takes me about three seconds to pull that same information."

TAG Cyber: How does SecurityScorecard show a return on investment in this cost sensitive environment? That is, how is it enabling customers and their businesses as required security investment?

SECURITYSCORECARD: Now more than ever, security teams need to collaborate effectively across their organization in order to bring value beyond their own team. By working cross functionally, SecurityScorecard enables businesses to make security a winning team sport. Features like our letter rating and canned reports make it easy for non-technical members of an organization to understand cyber security risk. With SecurityScorecard, vendor risk managers onboard third parties 75% faster, legal ensures vendor security in contracts, revenue teams stand out against competition, finance optimizes the cost of cyber insurance, and executives quickly understand the ROI of cyber security initiatives.

AN INTERVIEW WITH WITH MICKEY BRESMAN, CEO, SEMPERIS

CYBER RESILIENT IDENTITY ENVIRONMENTS FOR ENTERPRISE

The importance of Microsoft Active Directory (AD) in enterprise IT infrastructure is clearly understood by practitioners—and this has extended more recently to security teams. Much of this new security emphasis around identity and directory services has been on the potential for attackers to use infrastructure to accelerate enterprise breach campaigns. This usually involves increasing privileges through poorly configured AD deployments.

An often-overlooked threat, however, involves catastrophic breaks in directory services. These can originate from malicious attacks, and also more unintentional administrative mistakes. In either case, the consequences can be severe, often requiring lengthy periods of recovery and restoration. Any enterprise practitioner will immediately understand the implications of directory service outages. In most cases, the entire business will operate in a severely degraded mode.

The TAG Cyber team recently sat down with an expert in this area. Mickey Bresman, CEO of New York-based Semperis, explained to us how his team offers Active Directory recovery services, along with protective capabilities that help customers avoid the identity and challenges referenced above. As should be evidence in the interview below, Mickey emphasized how automation plays a critical role in the resilience process.

TAG Cyber: What are the primary threats to Active Directory that your team addresses?

SEMPERIS: In my conversations with security executives and practitioners alike, AD is frequently referred to as the "Achilles' heel" of enterprise security. Not only does it hold the keys to the kingdom—it's a treasure map for attackers. And being fundamental to the IT infrastructure, if AD is encrypted or wiped out, business comes to a screeching halt. Unfortunately, AD is very difficult to secure, given its constant flux, the sheer number of settings, and the attackers' easy access to powerful hacking and discovery tools. Further, ransomware attacks have quickly evolved into highly targeted and extremely damaging network-wide infections that can proliferate through AD. To put it plainly, AD was built 20 years ago, and although it stood the test of time, it can't stand up against today's threats on its own.

In our mobile-first, cloud-first world, any connected device can expose the heart of your IT infrastructure. In fact, you should assume that attackers are already lurking inside of your AD and just waiting for the opportune moment to strike. With this in mind, defenders must anticipate their adversaries' advances and thwart off AD attacks at every stage of the cyber kill chain. Semperis delivers comprehensive threat mitigation and cyber resilience for AD. Our patented technology for AD protects over 40 million identities from cyber attacks, data breaches, and operational errors. We deliver defense in depth across the full attack continuum—before, during, and after an attack.

TAG Cyber: Tell us about the algorithms you use to accomplish this recovery and protection. How do they work?

SEMPERIS: A typical Active Directory is in a constant state of flux, with hundreds or even thousands of changes made each day, which makes securing AD a proverbial "moving target." To maintain control of AD, monitoring must occur on two fronts: (1) security posture of AD (how objects are configured in AD to protect against attacks) must be monitored, and (2) changes to AD must be monitored with the ability to auto-remediate sensitive changes for round-the-clock protection.

Semperis continuously monitors for indicators of exposure and also consumes the AD replication stream and native Windows security event logs to capture changes to AD that could result in security compromises. Semperis monitors all aspects of AD, including integrated DNS, Group Policy, sites, and subnets, etc. The unique part of our approach is in the completeness of the solution. In the pre-attack stage, we provide our customers with new templates of indicators on a continues basis. Semperis offers customers built-in threat intelligence from a community of security researchers—our own and from the general community. If a new type of an attack vector is discovered, we will provide customers with a new template to simply import via PowerShell and from that moment on, the system will monitor for the new threat.

On the disaster recovery side, Semperis introduced the first backup and recovery solution purpose-built to recover AD from cyber disasters like ransomware and wiper attacks. When your business is down, every second counts and complexity is your enemy. Semperis fully automates the AD forest recovery process to avoid human errors and reduce downtime to minutes instead of days or even weeks. Our patented technology separates AD from the underlying Windows OS and only restores what's needed for the server's role as a DC, DNS server, DHCP server, etc. —virtually eliminating the risk of malware re-infection during restore.

TAG Cyber: Do you see much difference between malicious attacks on Active Directory and inadvertent administrative errors? Do they have the same potential impact?

SEMPERIS: Yes, there is a big difference between the two. From my perspective it comes down to trust. Do you know what hit you? Do you trust your backup? How about the Windows that your AD is running on?

In the administrator error scenario, you know (hopefully) what happened and can reuse parts of your infrastructure. In the malicious attack scenario, you can't trust Windows, and if your backup includes big parts of Windows (like in the case of system state and bare metal), you can't trust your backup either. We

And being fundamental to the IT infrastructure, if AD is encrypted or wiped out, business comes to a screeching halt.

have witnessed scenarios where the organization will spend days to restore AD, just for it to go down again soon after the recovery. So, although the damage of downtime is as painful in both scenarios, recovering from a malicious attack requires a different approach. Also, keeping in mind that a malicious attack might mean that the attacker has hold in your AD (privileged accounts) and not just the Windows (malware).

As the cyber threat became the much more common scenario, by default we assume the worst in our approach to recovery, with a share nothing, trust nothing state of mind.

TAG Cyber: What are some of the restoration improvements you see for enterprise customers? How much more quickly can they recover after a problem?

SEMPERIS: Semperis puts AD recovery on autopilot, empowering customers to respond more effectively to security incidents and everyday operational mistakes. With Semperis, customers shorten the recovery time of their entire AD forest by up to 90%. Being a fully automated solution, Semperis removes the dependence on resource-intensive and error-prone operations. We pride ourselves on delivering the fastest, safest, and easiest AD recovery solution on the market. The solution's end-to-end automation orchestration process frees up teams to allocate more focus on other aspects of the business. Here's one of our favorite customer quotes from the InfoSec Identity and Directory Lead at a F100 Global Retailer: "When I saw the Semperis solution for the first time, it nearly brought tears of joy to my eyes. It is exactly what I hoped for in an AD recovery tool. Over the years, I've had numerous concerns about forest recovery, and Semperis addresses them all."

TAG Cyber: Is real-time visibility into directory service infrastructure one of the benefits of your solution?

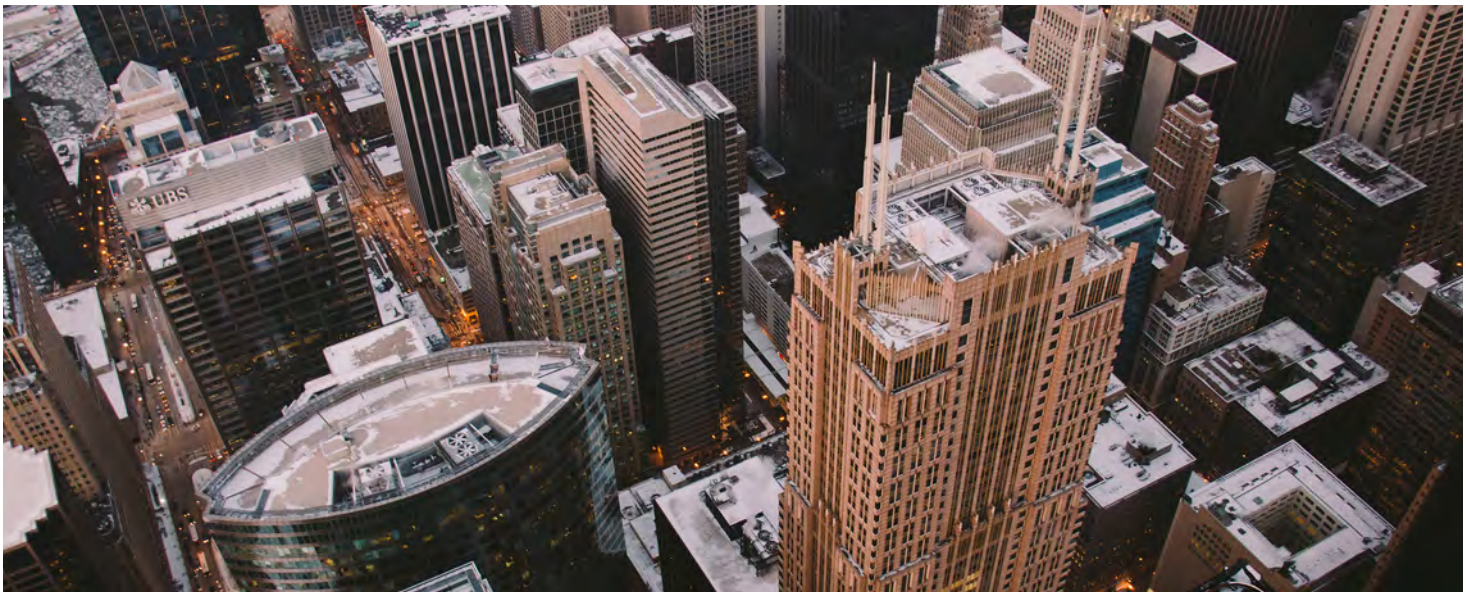
SEMPERIS: An attacker seeking persistent privileged access in Active Directory will typically attempt to bypass security auditing in some way. Security and auditing solutions like SIEM rely on either a native auditing agent on every domain controller (DC) or on security event logs (or both). But an attacker can circumvent auditing in any number of ways, including deleting the event log, stopping the collection agent, and turning off auditing. Sophisticated attacks can also bypass security auditing altogether. For example, the DCShadow attack technique injects changes directly into the AD replication stream.

Semperis leverages multiple data sources, including the AD replication stream, to provide uninterrupted visibility and capture changes that otherwise will go unnoticed. So even if the change was made while the auditing agent on the DC was down, and

even if the security event logs were destroyed, our customers will still have the visibility into the modifications made in the environment. On top of that, we provide the auto remediation capability, where the system can take the decisions to undo a change or take an action like disable an account and have the security analyst investigate.

TAG Cyber: Any final thoughts on the future of identity and directory service integrity and resilience for enterprise?

SEMPERIS: Organizations are going through a massive digitalization change. Software as a service adoption, WFH, BYOD, and other business trends changed the IT security concept of being in the same perimeter, behind a firewall, with organizational policy on the organizational devices. Many have said that identity is the new perimeter in this new world and I couldn't agree more. In Semperis we believe that world is going to be hybrid for a very long time, with line-of-business applications running both in the data center and being adopted as a service. Hybrid scenarios and cross cloud scenarios (using Box with O365, for example), will be dominant in the future. In this new world, protecting identity across multiple providers will be crucial to the organization's security, compliance, and operation. Identity is already a command and control in many aspects, but also a lucrative target for an adversary ("keys to the kingdom"). We want to make sure it's secured, protected, and can be easily recovered in the worst-case scenario, no matter where the attack came from or how severe was the damage.



AN INTERVIEW WITH WITH MIGO KEDEM, SENIOR DIRECTOR, PRODUCTS & MARKETING, SENTINELONE

UNIFYING ENDPOINT SECURITY FOR ENTERPRISE

The importance of endpoint security in the context of emerging zero trust security is clearly recognized—and this is reflected in the growing number of choices enterprise teams have in the selection of a suitable endpoint protection solution. Commercial tools focused on prevention, on detection, or on the related functions of remediation and response are readily available—and this can lead to confusion for enterprise teams.

A new goal has thus emerged to unify and introduce greater commonality for the required endpoint security functions in an enterprise. The goal of uniting prevention, detection, and response has therefore become an important priority—and this is not just for management simplification. It also increases the effectiveness of the endpoint controls and can help reduce operating and capital expense investments by the security group. Having a solution capable of distributing intelligence and coordination actions across the prevent, detect, and respond lifecycle—regardless of attack surface— is extremely powerful for a SOC.

The TAG Cyber team recently sat down with Migo Kedem of SentinelOne to learn more about how the company is working to unite and unify endpoint security into a next-generation cyber security platform that can address many of the goals mentioned above.

TAG Cyber: What's promoted the increase in attention to endpoint security in our community?

SENTINELONE: Endpoints were always a lucrative target for cyber attacks, and the reasons are simple: It's where we work, and humans are vulnerable from a cyber security perspective. For those who work in an enterprise, it's also where we access, and in many cases store, the data we use and produce to do our jobs. These elements always drive cyber criminals to invest in compromising endpoints. Gaining access to a single endpoint is the key to breaching the enterprise.

TAG Cyber: Do you see unification of endpoint security functions as a requirement coming directly from practitioners?

SENTINELONE: Yes, 100%. Especially since COVID, we see a change in how enterprises allocate budgets, and the consolidation of tools is one of the easiest ways to reduce cost without compromising on security. Automation also helps cut down the inherent costs of responding and investing in manual work. More tools means more labor to manage them, which translates to cost. Solutions which consolidate and automate are getting moved to the top of CISO spending.

TAG Cyber: Tell us about your platform. How does it work?

SENTINELONE: The journey of the SentinelOne product is unique. Even at the beginning, the solution baked in EPP [endpoint protection

platforms] and EDR [endpoint detection and response] in a single architecture. Aside from our prevention and detection capabilities, we were the first to introduce the concept of rolling back a ransomware infection, so users who may have seen traces of infection could keep working.

In 2015, we introduced cyber insurance—a term not previously used by a vendor to say, "We are confident enough to stand behind our technology and we will pay if we miss a breach."

Over time, the platform evolved to answer the new needs of CISOs and security practitioners, like IoT discovery and cloud workload protection. We also introduced capabilities to support an easy switch from legacy AV suites commonly needed by enterprises, like device control (USB), Bluetooth control, and even endpoint firewall control.

The SentinelOne security platform's most significant evolution was when we introduced Singularity. In short, the platform combines all the capabilities mentioned above into a holistic platform so that enterprises can choose the right solution for their needs. This approach allows enterprises to install one agent, to manage it from a single console, and replace traditional AV with a much better AI-based solution that is cross-platform. It includes an EDR and XDR that allow for automated response (which means that security and incident response teams aren't fielding calls in the middle of the night); visibility into every asset on your physical and virtual networks; and vulnerability scanning, Bluetooth control, isolation of infected devices, and a long list of features to keep enterprises safe from cyber attacks while maintaining our original single agent and single management console architecture.

The hallmark of Singularity is that all this rich device and user data is stored in a data lake available to each of our customers. This takes SentinelOne beyond a unified EPP and EDR endpoint solution of choice—we also are an IoT security solution, a cloud security solution, and a security/data analytics company—all in one.

TAG Cyber: What trends do you see in the types of threats that endpoint tools are expected to mitigate?

SENTINELONE: Several new trends are affecting this market:

1. Ransomware is no longer a decryption play, but downright extortion. Highly organized crimeware groups (such as Dridex and Trickbot) once relied primarily on banking fraud and demonstrated success, utilizing ransomware as their primary attack vectors. Such operators are now using the same capabilities to compromise enterprises, not only to blindly encrypt devices (like the case of the City of Baltimore which

Solutions which consolidate and automate are getting moved to the top of CISO spending

cost $17 million in recovery), but to exfiltrate data, post demands on public websites, and to hand data back only after receiving the ransom. The economics of this trend should alert all security practitioners: Enterprises risk facing substantial financial damage by either collaborating with crimeware groups or by having their PII and customer data exposed to the public.

2. The scale of operation and the use of AI. There is no doubt that the capabilities of AI are allowing all kinds of technologies to be more effective. AI has become more accessible to different types of organizations, and at the same time, it has become available to organized crimeware groups. This means that defending using AI is not a luxury but a necessity. Attacks are more lethal and debilitating than ever before, given that the adversary uses AI just like defenders.

3. Ransomware-as-a-Service – Heaven's gate to criminals. In the past, the bar of creating ransomware for profit was much higher than it is today. This changed in recent years. While Ransomware-as-a-Service does not change the way to defend, it exponentially increases the number of malicious attacks seen today by businesses of all sizes.

TAG Cyber: Is proper use of artificial intelligence an important factor in the success of an endpoint security solution?

SENTINELONE: Artificial intelligence is a critical element in the fight against malicious threat actors. It is definitely not a silver bullet, but it is a gateway to efficiency and automation. If you ask any AI experts, they will all say the same—the quality of AI-driven security protection is as good as the data you use to train AI. Knowledge accumulated over time helps companies incorporating AI to understand the blind spots of AI. In addition, as mentioned before, the democratization of AI—meaning, it's being used effectively by both defenders and attackers—has created the reality that using AI is no longer a differentiator, but a baseline of a security stack.

TAG Cyber: Any final predictions about endpoint security and endpoint-related threats?

SENTINELONE: Yes—securing enterprises is an ever-changing battle to overcome threat actors. Today, standing still is effectively moving backwards. The economics of malware, and specifically ransomware, still fuels a vast criminal market that sometimes operates like startups that are capable of innovating and taking advantage of fragmented and vulnerable networks (remote work is one example).

To adequately protect against such challenges, one needs to find a security solution that is trusted and proven in the wild, without creating more burden on the existing cyber security workforce.

These inherent challenges are not going to lessen in the future; on the contrary—we keep adding more and more devices that access our networks and data. By doing so, we increase the attack surface, sometimes without realizing or considering the implications. You don't find many enterprises capable of coping with this real-world challenge—this is where technology helps close the gaps.

In summary, the need to protect devices of all kinds grows; the challenge—and opportunity—is increasing protection and visibility without impacting overhead and human capacity to manage the evolving and complex enterprise architectures of today and tomorrow.

AN INTERVIEW WITH WITH YOSSI APPLEBAUM, CEO, SEPIO SYSTEMS INC.

DON'T FORGET THE PHYSICAL LAYER IN YOUR SECURITY STRATEGY

When many companies are choosing to migrate on-premises data centers to cloud environments, it's easy to forget that hardware is still prevalent in the enterprise. From laptops to mobile and IoT devices, there are more physical things communicating with corporate networks than ever before. And in a world where hardware supply chains are diverse and distributed, plenty of opportunity for hardware manipulation exists, threatening to compromise organization's networks once connected. Because hardware is comprised of multiple components, any one of which could offer a vulnerability, rogue device detection and behavioral monitoring are critical for risk reduction.

We spoke with Yossi Applebaum, CEO of Sepio Systems Inc., about detection and mitigation of rogue devices implanted onto hardware infrastructure and why, in a time when software dominates corporate environments, hardware risk must be a priority for the CISO.

TAG Cyber: Why is hardware compromise so much harder for enterprises to identify?

SEPIO: Rogue devices can attack the endpoint or the network. Manipulated USB HIDs (human interface devices) which target the endpoint not only appear genuine to the human eye but are recognized as legitimate HIDs, such as a mouse or a keyboard, and therefore are not identified as suspicious by security software solutions. Network Implants target the physical layer which security software—mainly NAC and IDS—do not cover. Again, alarms are not raised, as there is no detection of a suspicious device. The attack itself will need to be discovered for an enterprise to realize that they are a victim. Still, it can be a tedious process to discover the origin of the hardware attack and whether other devices have been manipulated.

TAG Cyber: Please explain how Sepio's solution handles rogue device or tampered device detection. What is your version of fingerprinting?

SEPIO: Sepio Systems calculates a digital fingerprint using the device descriptors of all connected peripherals and compares them against a known set of malicious devices, automatically blocking any attacks. Our software uses machine learning to analyze device behavior to identify abnormalities, such as a mouse acting like a keyboard. In addition to the deep visibility layer, a comprehensive policy enforcement mechanism recommends on best practice policy and allows the administrator to define a strict or more granular set of rules for the system to enforce.

Sepio Network Security works at the physical layer, polling switches to analyze what is happening at that layer and detecting all rogue devices plugged into the ethernet network.

Sepio Endpoint Protection guards against rogue devices connected to USB ports through multiple security layers, including real-time behavior analysis of suspicious devices. A rogue device being used to carry out an attack would be detected and blocked.

SepioPrime orchestrates Sepio's solution and presents the overall status and security dashboards. It also alerts for security threats, defines and distributes the device usage policies, and delivers risk insights and best practices recommendations.

TAG Cyber: With cloud taking over, which industries still need to pay extra attention to trustworthy hardware?

SEPIO: In short, all industries need to be aware of the risks of hardware. Industries cannot assume that making use of the cloud eliminates all hardware risks. When one door closes, another one opens, and although migrating to the cloud reduces the risk of attacks on a physical data center, the cloud brings new hardware vulnerabilities that malicious actors are looking to exploit. Moving over to the cloud means that there are more devices which can access the data from anywhere in the world, at any time, thereby increasing the number of entry points for a perpetrator to target with manipulated hardware.

Some devices used to access the cloud might have few security features, such as IoT devices and employees' personal devices, thereby making them easier for attackers to target and, as a result, can provide attackers with access to the cloud. In summary, when talking about HID attacks, the attack tools impersonate a human operator, and as such, it is less important if the attacker is accessing the data through a cloud connection or a physical local machine. The result is the same.

TAG Cyber: How does a solution like Sepio complement application-layer security hardening?

SEPIO: Sepio's solution provides enterprises with a more comprehensive understanding of their IT assets by providing protection on the physical layer. This means that no device goes undetected, whether it's a USB gadget or an unmanaged ethernet switch. There is no longer a need to rely on manual reporting, legacy inventory reports, and employee compliance to determine if there is a vulnerable device installed by an over-eager employee with good intentions, or through a compromised supply chain. Ultimately, enterprises with application-layer security that also implement Sepio's solution can be sure they have the most extensive cyber security features available and, in turn, a stronger cyber security posture with multi-layer security coverage.

TAG Cyber: How does the new everyone-work-from-home paradigm change the approach to physical layer security?

SEPIO: Sepio Systems' research team has been examining the effect of work from home during these past months; the data for this analysis was collected from our Sepio Cloud service, which managed

large volumes of endpoints with their peripheral devices and accessories.

We found that there was an increase of 42% in the number of devices connected to corporate endpoints compared with the pre-COVID-19 period. That said, it is not only the number of connected devices that is important to note, but also the fact that we now see almost three times the number of different device vendors—many of which are no-brand, unrecognized, cheap devices that are not common in the enterprise environment. This significant rise is attributed to the fact that employees are connecting their existing home peripherals to their endpoints. From selected inquiries we made, we saw cases where the enterprise's endpoint was used by other family members for remote schooling or just for fun and games.

Another interesting observation is the fact that operation hours were significantly extended, so where we once used to see standard office working hours, we now see those standards being stretched as the boundaries between work and leisure hours are mixed together. This creates a new "normal," which is hard to baseline as of yet.

Working from home trends have been rising in popularity, even if we look at trends from pre-winter/spring 2020; seventy percent of people work remotely at least once a week, and over 50% of people work remotely for at least half of the week. Today, COVID-19 is essentially forcing many businesses to make the temporary shift to remote work for everyone, meaning more employees are working at home and fewer, if any, are in the office. Working from home means that here are numerous devices connected to the corporate network with a range of manufacturers, and each with different functionalities and capabilities. Although CISOs have started to create longer term security strategies, they sometimes fail to consider peripherals such as keyboards, mice, and USB charging cables, as they are not considered vulnerable devices.

Industries cannot assume that making use of the cloud eliminates all hardware risks. When one door closes, another one opens.

However, these devices do pose a threat to the organization, as they have the functionality to both insert and extract, giving them the capacity to cause damage, should they be instructed to do so, even remotely through spoofed wireless connections. These hardware devices can be imbedded with microcomputers, such

as the Raspberry Pi, and manipulated to act with malicious intent through payloads. Hence, malware might be installed in the form of Trojans, worms, or viruses. Other attacks such as man-in-the-middle (MiTM), distributed denial of service (DDoS), keylogging, and data breaches can also take place via this attack vector. Moreover, these attacks can be carried out in minutes, if not seconds, and, even after the device has been removed, attackers maintain remote access to the organization's network, allowing them to move laterally and gain further access to confidential data.

Ultimately, organizations need to be more aware of physical layer security since work from home policies present an even greater risk of hardware attacks. The approach to physical layer security now needs to be much more proactive since enterprises have less control over what peripherals their employees are using when working outside of the office, and who actually has access to the organization's assets.

AN INTERVIEW WITH WITH GREG TAYLOR, CEO & PRESIDENT, SERTAINTY

SELF-PROTECTING, SELF-AWARE DATA

Data is often considered the "crown jewels" of business operations. From intellectual property to customer records and financial information, organizations must covet data and ensure its confidentiality, integrity, and availability. For years, cyber security practitioners have touted the advantages of placing the strongest controls directly around data, yet the difficulty in doing so has led to additional compensating controls farther and farther away from the data itself.

In more recent years, as zero trust has moved beyond theory and into organizations' architectural plans, data has once again become the focus—whether it's endpoint controls aimed at preventing end devices from reaching sensitive data stores or web application firewalls that monitor and block traffic to the applications that contain the important data.

One company has taken a different approach; Sertainty has maintained a laser focus on data protection, building a so-called "self-protecting-data" platform. We spoke with Eric Rickard, President at Sertainty, about their technology and why it's important to control access to data inside files as well as throughout the network.

TAG Cyber: Can you frame the scope of data loss and data leakage for enterprise organizations?

SERTAINTY: Well, that'd be an enormous frame, and translates into an enormous opportunity! General Keith Alexander is on record saying that trillions of dollars of intellectual property is siphoned out of our nation on an annual basis. That's discerning enough. But I believe an even more destructive threat to our nation and a critical issue for enterprises is the illicit harvesting of personal data and the compromise of citizen privacy.

Getting back to the "enormous opportunity," if I may: The Sertainty opportunity in the global cyber security market is an incalculable green field. Who could argue, since nearly every known cyber security solution has failed to prevent data breaches? Sertainty makes data loss irrelevant. Perhaps more impressively, self-protecting-data solutions also generate new revenue streams for our customers!

TAG Cyber: What, exactly, is "self-protecting-data"?

SERTAINTY: Our approach to data protection employs three themes; first, we irreversibly couple data protection schema with data governance. Second, we irreversibly couple intelligent decisioning with the controls. And third, we irreversibly embed this "intelligence" in the data file. We sometimes use the term "intelligent data."

To use an analogy, imagine four decks of sports memorabilia cards, for example baseball, football, soccer, and basketball cards. These decks represent the different data types in our self-protecting-data. Imagine the baseball cards represent some access control logic and a tiny computer application, … sort of a "nano-defense module." This deck will eventually

be shuffled, but for now, mentally set it aside.

Now, imagine the football cards represent the data to be protected, and the soccer cards represent all the encryption keys to the protected football data. Lastly, the basketball cards represent the digital identities of the persons or devices that are authorized to access the football card data. Now mentally shuffle each of the individual decks to emulate encryption, then cut each deck a few times to add some randomness to the shuffle. We'll call this "hyper-fragmentation."

Next, mentally combine the decks and shuffle them together with more hyper-fragmentation. Finally, split the deck and insert the baseball cards (i.e., access control logic and nano-protection module), shuffle the four combined decks, and hyper-fragment them one more time.

The elegance and simplicity of this patented data protection method is evident. The data and all the necessary security apparatus are locked in a secure, randomized, multi-segmented, multi-layered data object. Brute force attacks simply cannot reverse this process. However, access to the right information, at the right time, in the right place, typically in milliseconds, for the right (authorized) persons or devices is transparent. Better yet, the data has no reliance on external security mechanisms.

TAG Cyber: Why wouldn't encryption be enough? In thinking about that, one of the longtime problems with data protection technologies has been data classification. Companies often don't know what data they have, where it resides, who owns it, etc. How does Sertainty change that dynamic?

SERTAINTY: From a CISO's perspective, Sertainty intelligent data resolves the last unsolved cyber security challenge—protecting data everywhere and forever. The foundation of zero trust architectures (ZTA) demands self-protecting and self-aware data—intelligent data.

The foundation of zero trust architectures (ZTA) demands self-protecting and self-aware data—intelligent data.

From a regulatory compliance perspective, intelligent data is also self-regulating. Better than mere encryption, self-regulating-data resolves the enormous problem of irrefutably recording how, when, where, and who accessed the data at the file level.

From an operating officer's perspective, self-protection and self-regulation means that digital assets are always accounted for and available to be monetized. Consequently, customers recognize the impact of intelligent data solutions' affordability and effectiveness by unifying digital asset protection, digital inventory management, digital regulatory compliance, audit, and digital consumer behavior understanding. Sertainty took what began as a data security concept and monetized zero trust to

zero cost.

TAG Cyber: What do you mean by "zero trust meets zero cost"?

SERTAINTY: Market feedback has revealed an unexpected result. Part of being self-protecting requires the data to be self-aware. Being self-aware meant it could be self-reporting. Organizations that employ Sertainty technology are not only secure, but their files can report who, where, and when access is attempted, authorized, or denied. By aggregating data file event logs companies get absolute data security, automated consumer behavior analysis, and cost reductions through automated and irrefutable regulatory compliance reporting. For companies who care about security and revenue, Sertainty enables automated regulatory compliance validation (e.g., GDPR, HIPPA), assured payment for subscription data services (e.g., Wall Street Journal), and consumer behavior analytics (e.g., Sony). Without exaggeration, the global impact of intelligent data (zero trust at the data-layer) is incalculable.

AN INTERVIEW WITH WITH BOB LAM,
CEO & CO-FOUNDER, SHARDSECURE

ZERO DATA SENSITIVITY WITH MICROSHARDING

What's the best way to ensure data security and privacy in the cloud? The obvious answer is encryption. Why, then, do a majority of companies fail to encrypt their data? Maybe it's a misunderstanding of the Shared Responsibility Model, or maybe it's because traditional encryption is time-consuming, highly manual, and expensive.

If the risk of compromise weren't worrisome enough, compliance mandates now require companies to place additional controls around sensitive data for privacy purposes and to segment data, making the data harder for cyber criminals to see if they gain illicit access to the environment. Encryption, stronger data access controls, and least privilege are industry best practices, but none of these has yet reached the level of ubiquity necessary to meet mandates in all cases, or protect organizations from breach—as we've seen time and time again. We spoke with Bob Lam, CEO & Co-Founder at ShardSecure, about their Microshard data security solutions and how microsharding can enable cloud adoption and improve data security across hybrid cloud environments.

TAG Cyber: First off, what is Microshard technology?

SHARDSECURE: Sharding has been around for a long time. It is used to split datasets into smaller fragments to improve performance and resilience. Dropbox shards their data into 4MB each while others shard data down to the kilobyte level. Even a 1 kilobyte fragment, though, is large enough to contain 111 Social Security Numbers. Our patent-pending technology is innovative because we break data into single-digit bytes (hence the term Microshards) which become too tiny to be valuable to any malicious actors. Additionally, with parallel reads and writes, particularly in a multi-cloud/multi-data-center environment, we can actually improve cloud speed and performance by 2-10x. In essence, we provide better and faster cloud data security solutions while giving our customers a positive ROI!

TAG Cyber: What is the advantage of Microsharding over traditional encryption, especially in the cloud?

SHARDSECURE: Great question! While encryption for data on premises only might be just good enough to protect data at rest, customers are faced with a new set of security, privacy, and regulatory risks as they move to the cloud, whether it's a hybrid cloud or multi-cloud environment.

Today, less than half of enterprise data in the cloud is encrypted. Why? First, encryption is no longer bullet proof in today's high-speed compute environment with faster and cheaper GPUs. It continues to drag on performance, particularly in the cloud, where there is also

But do you really want to trust your cloud providers with your keys in addition to your data?

latency to contend with. Encryption also adds significant complexity, friction, and management costs to the compute infrastructure, applications, and workflow. Lastly, the biggest challenge for encryption remains key management. Who should be managing your keys in the cloud? If you let AWS or Azure manage encryption keys for you, it's cheap and simple! But do you really want to trust your cloud providers with your keys in addition to your data?

With Microsharding, we provide Absolute Privacy and Zero Data Sensitivity for our customers. Cloud misconfiguration remains a top cause for data breaches, and our technology significantly mitigates that risk. We also reduce organizations' attack surfaces and provide compensating controls for encryption to meet certain regulatory requirements. Our product looks like a virtual disk that can be deployed as a container or VM, both in the cloud or on-prem. We don't have the key management issues inherent to encryption, where you need to manage all the endpoints and re-encrypting the keys.

With ShardSecure, you don't need to choose between Microsharding and encryption, as you can layer our product on top of encryption to provide defense in depth, a solution many of our early adopters deploy. With the Zero Data Sensitivity provided by Microsharding, customers are more comfortable letting cloud providers handle encryption and key management while managing our ShardSecure virtual appliance on their own. Longer term, we do believe Microsharding can replace encryption as the dominant data security technology to secure data at rest in the cloud.

TAG Cyber: Tell us more about how Microshard technology works.

SHARDSECURE: Our ShardSecure software appliance breaks data into tiny fragments that can be as small as low-single-digit bytes, and false shards are added to further obscure data. Data is then distributed across multiple locations including local storage, AWS, Azure, Google Cloud, IBM, and Oracle Cloud.

Shard size, contaminated fragment quantity, and compression are all customizable according to the customer's unique security and performance requirements for each data set. Every new piece of data provides further obfuscation. ShardSecure is easy to deploy as a virtual machine or container either on-premises or in the cloud. The product looks like a virtual disk and is application-agnostic (supporting files, database, and streaming video). Microshard data is reassembled for legitimate users without sacrificing performance.

We have a policy-based engine that determines how and

where to distribute the shards, as well as the shard size, to give customers control over where the data goes. The size of the shards can depend on the data type—for example, streaming video files might become bigger shards than text files. Data can be streamed up and down, and we use caching and compression techniques to minimize latency and accelerate performance.

To reassemble the shards, we use pointers in our ShardSecure engine to determine where the data resides and reassemble the data into its original form provided that the requesting party knows all of the locations where the data has been distributed and has access to them. Importantly, we tokenize these pointers for an added layer of security, which also reduces latency, as tokenization effectively compresses the pointers. It is important to note that these locations are unrelated and not known to each other.

Fragmenting data into tiny elements which are spatially dispersed and intermixed with other fragments has numerous advantages in security and compliance. The fragment size can be chosen to statistically reduce or even eliminate the possibility of sensitive data and contextual metadata existing. This applies to both data at rest and, when the fragments are routed over multiple network paths, data in transit.

An attacker intercepting Microshard data has no way to put the pieces back together because they will always have an incomplete set. This is contrasted with encryption, in which the full set of data is compromised and needs to be unscrambled. Unscrambling data requires time and compute power. Reconstituting data fragments requires most or all of the data fragments, something the attacker cannot obtain without compromising all possible storage locations everywhere. We have effectively turned the attacker's challenge from a time and compute power problem to a time, compute power, and spatial problem. Encryption may slow an attacker down, but Microshard data protection persists over time. Faster computers won't help an attacker, not even quantum computers. You can't unscramble data that you don't have.

Additionally, the option to ensure that no single (or statistically meaningful) set of data fragments contains a full element of sensitive data has compliance benefits. Once the Microshard data elements no longer contain such information, the files in which they sit are no longer sensitive. Much like tokenized data no longer needs to be protected by policies governing sensitive information, Microshard data similarly has stripped the files of the elements that made them sensitive. There is no need to treat files that contain no meaningful, sensitive data as if they contained such information.

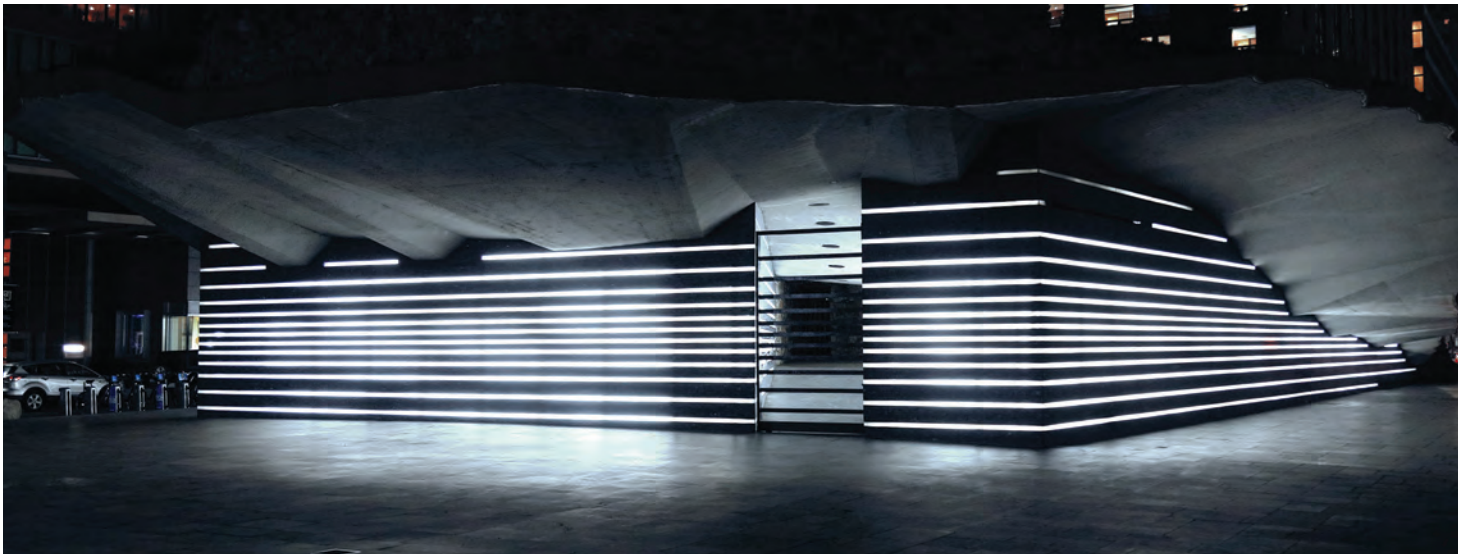
TAG Cyber: Most cloud security solutions look at the front end, but you emphasize ShardSecure as a back-end technology. What does that mean and why this approach?

SHARDSECURE: Large CASB and MFA vendors such as McAfee, Netskope, and Okta are doing a terrific job securing the access path to enterprise applications hosted in the public cloud (front end).

ShardSecure focuses on securing data on the back-end cloud infrastructure, where privileged cloud administrators perform important daily activities including patch management, software updates, and other critical tasks that bear serious consequences in the event of data breaches. Little attention has been paid to securing access to back-end cloud data, and Microshard technology is an excellent way to achieve zero trust in data security by separating sensitive data from privileged administrators, who could be compromised, disgruntled or simply make mistakes unintentionally that cause data breaches.

TAG Cyber: Is there a compliance angle to this?

SHARDSECURE: Absolutely. Microsharding eliminates data sensitivity and renders data completely unreadable in the event of a breach. Some of our early adopters are seeing savings in compliance and audit costs as some datasets are being reclassified to lower sensitivity class. We are in the process of educating regulatory authorities in both the US and EU on the value of Microshard technology and how it can help companies mitigate regulatory compliance risks presented by GDPR, CCPA, and the Cloud Act.



AN INTERVIEW WITH WITH ZANE LACKEY, CHIEF SECURITY OFFICER AND CO-FOUNDER, SIGNAL SCIENCES

REDUCING RISK AT THE APPLICATION AND API LAYERS

Firewall technology has undergone many updates and adaptations during its almost four decades of existence. What started in the 1980s as a way to keep unauthorized users outside the corporate perimeter, firewalls today must be able to handle cloud instances, container use, myriad mobile device types, and the predominance of software that allows businesses to function. Modern firewalls that place a ring around the network have their place, but they are not sufficient for protection of organizations' most-sensitive assets. That is: applications and the sensitive, private, and proprietary data inside them.

Today, software and applications dominate organizations' networks, making them juicy targets for cyber criminals. To keep pace with rapid build and deploy cycles inherent in DevOps, organizations need application protection that won't break or fall over with every new deployment or update. Web application firewalls have quickly become the go-to technology to meet this challenge, and we recently spoke with Zane Lackey, Chief Security Officer and Co-founder at Signal Sciences, about the current state of WAF technology.

TAG Cyber: What are some of the changes necessitating how companies protect their networks?

SIGNAL SCIENCES: Risk has shifted from the historical infrastructure and network layers out to the endpoint and up to the application layer. For most CISOs (myself included), our primary source of risk used to be at the infrastructure and network layer, while the application layer was mostly low risk. However, for enterprises today, the risk sits out at the endpoint (via phishing, malware, etc.) and up at the application layer. This is because the core of digital transformation is about changing the way enterprises interact with their customers, resulting in applications going from being simple marketing websites to, instead, becoming the primary way in which an enterprise interacts with its customers.

This trend has further accelerated with the current COVID-19 pandemic and resulting work from home policies. This environment has driven record traffic to web applications and APIs for business and customer processes, and accordingly, the need to cover the explosion in risk at the web and API layer.

TAG Cyber: What about DevOps, in particular, is changing the security paradigm?

SIGNAL SCIENCES: The rise of DevOps, in particular, has forced the security paradigm to shift from being a blocker to an enabler. By adopting DevOps, teams can be changing code and launching new versions of software as fast as they want. There is no time for tuning, false

positives, or sole reliance on managed services to change rules every time an application or API updates. A modern security paradigm is one that enables the speed of DevOps while tying into the SOC and DevOps toolchains to provide the visibility needed for additional key business stakeholders to be security self-sufficient.

TAG Cyber: What are some of the legacy concerns about deploying web application firewalls you hear when speaking with security infrastructure and operations teams?

SIGNAL SCIENCES: The problems with legacy web application firewalls (WAF) solutions that we experienced at Etsy [where we working before founding Signal Sciences]—and our peers experienced at other enterprise companies—is the reason we founded Signal Sciences. Legacy WAFs were built as hardware appliances solely for data centers and aren't natively built for the hybrid of cloud, data center, and containerized applications and APIs that an enterprise finds itself using today.

To get coverage over applications and APIs in an enterprise today means being able to cover not only datacenter applications, but also lift-and-shift cloud applications, net new cloud-native applications, as well as microservices, container-based APIs, and even serverless applications. Enterprises going through digital transformation have realized they need one web application and API protection solution that they can deploy across all environments.

Additionally, the legacy WAF approach to rules tuning and "learning periods" was built for a waterfall SDLC when apps changed only a few times a year—but development has accelerated dramatically given the rise of Agile DevOps and rapid iteration/release methodologies, resulting in ever-increasing false positive problems and significantly higher TCO.

The false-positive statistic we get to share with customers is that, as unbelievable as it sounds, 95% of our customers have Signal Sciences in full blocking mode for their production traffic. Compared to legacy WAFs where the WAF was typically always left in monitor mode due to the number of false positives, this becomes a genuine surprise and strategic success for our customers when they make the switch. The comparison we continually hear from customers who replaced their legacy WAFs with Signal Sciences is that we have done to legacy WAF what Crowdstrike, Cylance, and Carbon Black did to legacy anti-virus.

Lastly, legacy WAFs, especially CDN WAFs, have extremely high TCO. Given current circumstances where budgets are top of mind, providing WAF services only attached to extremely expensive CDN services, and then, often requiring yet another

The rise of DevOps, in particular, has forced the security paradigm to shift from being a blocker to an enabler.

layer of expense for managed services to try to stay on top of the continual false positives, is not cost-effective for security infrastructure and operations teams.

TAG Cyber: What surprises customers most—when comparing Signal Sciences to legacy solutions—about how your web application protection works?

SIGNAL SCIENCES: There are four key wins we hear from virtually every customer we work with:

- Works with any architecture that their organization use to develop and deploy their apps: We support the extensive mix of public cloud, hybrid cloud, service mesh, containers, serverless, datacenters, and numerous others that enterprises have today. Whether they're going through digital transformation, or a cloud or DevOps journey, we support 100+ cloud-native and data center platforms all managed through one central console for visibility and policy enforcement.
- Eliminates the legacy WAF false positive problem: Unlike legacy WAF where false positives were a constant battle resulting in the WAF being left in monitor mode, 95% of our customers use Signal Sciences in full blocking mode in production. Additionally, no Signal Sciences customers have an FTE dedicated to WAF tuning/maintenance, where at enterprise scale, legacy WAFs typically needed anywhere from 3-5 FTEs just to manage rules and false positives.
- Provides broad coverage across web application and API threats: In addition to NG-WAF, Signal Sciences customers use our solution for coverage over API security, advanced rate limiting, malicious bots, account takeover/credential stuffing, and DDoS.
- Empowers DevOps, Security, and Operations teams: By plugging into the DevOps and SIEM toolchains through services, such as Splunk, JIRA, PagerDuty, Slack, and others, we enable our customers to use their existing toolchains without having to deal with yet another vendor dashboard.

All these add up to customer success metrics you almost never see from a security company:

- 4 out of 5 enterprises who try Signal Sciences [through a POC] become customers
- A 98% customer retention rate
- A Net Promoter Score (NPS) of 80 compared to the industry average NPS of 6 for legacy WAF vendors, which, amusingly enough, is the same score as the rental car industry

TAG Cyber: Where do you see application security headed in the future?

SIGNAL SCIENCES: The volume of applications, APIs, and microservices have increased exponentially in the past decade, as well as the sensitivity of the data they provide. This is further accelerated with the current COVID-19 pandemic and work from home policies driving record traffic to web applications and APIs for business and customer processes. As a result, digital transformation is increasing in velocity at a speed we've never seen before, and accordingly, so is the need to cover the explosion in risk at the web and API layer, resulting in the following:

1. Traditional coverage areas of application security will continue to expand across broad application and API protection to include advanced rate limiting, API security, bot mitigation, account takeover/credential stuffing, zero trust, and DDoS mitigation—all under a unified solution with a single management console and full feature parity across any and all deployment methods.

2. The rate of new technology entering the enterprise has risen exponentially. The rise of APIs, containers, and serverless, and the increase in technology platforms across the enterprise means that in order to gain strategic coverage over web applications and APIs, businesses need a protection solution that can deploy anywhere that applications and APIs live. Web application and API protection in the future will be built around this fact, and whether an enterprise has apps in the data center, or a business unit embraces APIs, microservices, or serverless, the application security solutions companies use will be one that can deploy across all of these environments.

3. With the rise of DevOps forcing security to shift from being a blocker to an enabler, there is no time for tuning, false positives, or sole reliance on managed services to change rules every time an application or API updates. A modern application security solution enables the speed of DevOps while tying into the SOC and DevOps toolchains to provide the visibility needed for additional key business stakeholders.

AN INTERVIEW WITH WITH AISLING MACRUNNELS, CHIEF BUSINESS AND GROWTH OFFICER, SYNACK

A MISSION-READY PLATFORM FOR VULNERABILITY ELIMINATION

In a never-ending battle against cyber attackers, vulnerabilities, and new technologies, organizations' best bet at keeping adversaries off the network is continuous testing and continuous monitoring. In the past, continuous vulnerability scanning and regular penetration tests conducted by a combination of internal and external experts were considered the gold standard. But in recent years, companies have realized that continuous scanning coupled with testing by a few, select researchers wasn't enough. Human bias played too big a part in whether certain vulnerabilities were found.

With the gig economy going strong and crowdsourcing becoming the accepted way to look for everything from your new favorite restaurant to avoiding traffic jams, a few innovative companies applied the idea of crowdsourcing to pen testing, combined it with automation and AI, and now offer full-service platforms to help companies test for and remediate vulnerabilities. Synack, a leading crowdsourced security provider, has a multi-dimensional solution. Aisling MacRunnels, Chief Business and Growth Officer, spoke with us about the market recently.

TAG Cyber: We keep hearing more and more from CISOs that they are substituting crowdsourced security testing for traditional pen testing. Please tell us why crowdsourced testing is becoming so popular?

SYNACK: We've seen a rise in popularity, simply put, because crowdsourced testing provided superior results in a space that badly needed a better solution. Not only are the results better at finding more vulnerabilities, but the on-demand deployments, the detailed actionable reports, and ongoing triage make it a much more competitive offering. Basically, the traditional models of security testing were not built to address today's dynamic, remote security needs. With a growing cyber talent gap (>3.5M jobs expected to be unfilled in the next year) and continuous development cycles, modern security teams require a more elastic solution. Crowdsourcing has risen in popularity over the last decade, and the crowdsourced security market has been born. However, as you've alluded to, the market is growing quickly and there are different forms of crowdsourcing solutions available today. Some, like bug bounty, take more of a broad marketplace approach where they match hackers with customers. Synack has taken a platform-driven approach where we enable our crowd with technology and provide a scalable, on-demand SaaS solution to customers.

TAG Cyber: I know you can't disclose any information about customer engagements, but what trends are you seeing in your researchers' findings? Are they different than last year?

SYNACK: This year is certainly different from last year in many respects—however, we are very fortunate in that the nature of our business has remained unchanged. In fact, it's growing. Crowdsourcing platforms were built for today's virtual working environments, and as a result, researcher engagement has been high. Over the last six months, we have seen an uptick in vulnerabilities discovered by our Synack Red Team (SRT). For example, activity by the SRT has increased by 70% during the COVID outbreak as work from home requirements and social distancing have translated into more time spent hunting for vulnerabilities (and more business and assets for Synack to test).

As many organizations have transitioned work to remote environments, new attack surfaces and, in some cases, new vulnerabilities are emerging. The most common types of vulnerabilities we have found are cross-site scripting, SQL injection, and authorization/authentication flaws. Furthermore, in the industry as a whole, we've also seen a lot of COVID-19-related malicious cyber activity like malware, phishing attacks, and attacks against newly- and often rapidly-deployed remote access and teleworking infrastructure.

TAG Cyber: Your platform goes beyond pen testing. Can you explain the different components of the platform and an engagement?

SYNACK: Synack started the crowdsourced security testing industry based on a belief that there was more to penetration testing than a checklist, more to testing technology than a simple scanner, and more to crowdsourcing than bug bounty.

How we engage is through a single platform built for scalable solutions. One of the primary challenges that a CISO faces is not security related at all—it's vendor management. We try to make our customers' lives easier by combining penetration testing, bounty-driven vulnerability discovery, compliance, and application security into a single, SaaS-based crowdsourced security platform comprised of:

- Synack Red Team: The world's best security researchers (vetted for both skill and trust) to provide adversarial insights
- SmartScan: AI/ML-enabled scanning technology to continuously monitor dynamic attack surfaces for potential vulnerabilities
- LaunchPoint: Our secure testing gateway that provides full testing visibility and control to the customer

Basically, the traditional models of security testing were not built to address today's dynamic, remote security needs.

- Centralized Management: Our in-house Synack Operations Team who manages testing end-to-end and triages all vulnerabilities to ensure that only actionable results are passed to the customer
- Client Portal: SaaS portal that shares real-time insights and analytics on testing performance
- Customized Reporting: Detailed reports are easy to understand and audit ready
- Integrated Platform: Centralized platform to manage and orchestrate security testing at scale

Few solutions provide both effectiveness and efficiency that the Synack platform provides. The

competitive landscape includes traditional consulting pen testing companies, bug bounties, and automated scanners. With Synack, it's all executed through one platform.

TAG Cyber: What are some of the objections you hear from CISOs who are reluctant to use a crowdsourced platform?

SYNACK: From the CISOs in our crowd, we tend to hear more questions over objections. CISOs want to ensure that they are getting everything they got before, all of the features they now need for the fast-paced, diverse environment we're living in today, and without increasing risk. Honestly, at Synack we find it's pretty easy to address all the CISOs' questions and we usually become a tight team with the customer's security team pretty quickly, while addressing legal questions.

TAG Cyber: We hear about the talent shortage all the time in security. How do you find elite hackers in this environment?

SYNACK: Our hackers are part of our IP. They are extremely important to us. We treat our elite hackers as part of the team. Respect is critical when you have the benefit of working with these enormously talented people. Now, although the in-person and event landscape has changed, we're finding unique ways to engage and promote the great work of the SRT. We track all the best security research around the world while also recruiting the "best of the best" security researchers and ethical hackers to Synack's Red Team. Synack runs various Capture the Flag (CTF) competitions and hacker hangouts around the world (currently virtual) to identify rising stars and bring them into the Synack community.

Synack only accepts the best and the most trustworthy ethical hackers and we believe there are only a few thousand of these types of people in the world. We only want the best on the SRT. Another really important factor is optimizing the size of the crowd to meet the market needs. When these ethical hackers spend

time on an asset, you want them to have an opportunity to make money, otherwise they get frustrated. We believe in the quality over quantity approach to deploy the right crowd.

We're lucky to have a waitlist of experts vs. the challenge of a shortage, and we continue to celebrate the hard work of the SRT through various programs, like our recognition program to get the SRT excited and engaged.

We recently launched a new initiative to recognize and celebrate the world's best hackers, the Synack Acropolis. The Acropolis is a beacon of trust, honor, and excellence that recognizes the best SRT for their accomplishments on the Synack platform.

We also have a strong veterans' program. We strive to recruit qualified veterans, empower them with the right tools, and deploy them on our testing platform. Based on their years of experience and service, many veterans are mission-ready and excellent candidates to join the Synack Red Team.

AN INTERVIEW WITH WITH TOM BADDERS, SR. PRODUCT MANAGER, TELOS CORPORATION

A VIRTUAL OBFUSCATION NETWORK TO SECURE THE INTERNET AND PROVIDE PERSONAL PRIVACY

What we now know as the internet was initially designed as an "information superhighway" by a collection of forward-thinking researchers, engineers, and programmers who wanted to provide greater facilitation of information sharing. It's unlikely that when the groundwork was laid all those decades ago, the inventors could have imagined the way in which people today create, share, and find information on the web via the internet. The open nature of the web, powered by the vastness of the internet, allows someone in Iceland to easily communicate and share information with someone in South Africa. But it's this same openness and complexity in networking that allows cyber criminals to use the internet to do nefarious things.

In today's globally connected world, individuals and enterprises need reliable ways to ensure their internet/web use is secure and private. Obfuscation and encryption have become powerful ways to ensure legitimate users' actions are not tracked or hijacked by cyber criminals. Though criminals can and do use the same tactics to commit crimes, Telos, a network security company based out of Virginia, is on a mission to ensure the bad guys don't have the upper hand on the internet. We spoke with Senior Product Manager, Tom Badders, about how enterprises can remain safe in a world of open and rapid digital communications.

TAG Cyber: The last five years of Telos' history are fascinating. Tom, please tell us about the company's evolution and how it led to the development of Ghost.

TELOS: These last few years have brought about a massive movement of enterprise network capabilities to the cloud. Telos has long been of the opinion that the cloud can provide better security and more resistance to cyber attacks than a premises-based network. With the knowledge that this movement to the cloud was inevitable, Telos long ago began evolving its flagship product, Xacta, to not only be cloud-based itself, but also to ensure our government customers were ready to move to the cloud from a risk and compliance perspective.

Further, leveraging the cloud requires the use of the internet to deliver data from corporate offices and remote workers to secure cloud repositories and back; in effect, the cloud and the internet have become part of the new corporate enterprise network. Private VPNs, firewalls, and other edge network security measures were not effective in preventing cyber criminals from getting into corporate networks, stealing private information, holding organizations hostage, or exacting an array of other attacks.

As the industry focused on securing the edge and the endpoint, Telos saw a need to focus on securing the internet itself. To

create true end-to-end security to eliminate attack vectors of cyber criminals. To not only protect the data traversing the internet, but also protect the identity and location of users and their organization. This product became Telos Ghost.

TAG Cyber: At a surface level, Ghost is a virtual obfuscation network. Although traditional obfuscation is probably well known to our readers, how is Ghost different and what, exactly, is a virtual obfuscation network

TELOS: Typically when one hears or reads about obfuscation, one thinks about data or code obfuscation. Specifically, data masking to hide original data with modified content to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data. Alternatively, code obfuscation is the deliberate act of creating source or machine code that is difficult for humans to understand.

By contrast, Telos Ghost is a virtual obfuscation network, provided as a service. It uses high levels of obfuscation techniques to conceal the presence of the network itself as well as the people and activity on the network—by varying network pathways, allowing customers to select various points of presence around the world, adding and removing source and destination IP addresses, as well as allowing customers to manage the levels of attribution necessary for their specific objectives. Telos Ghost is a private network that can be created to allow multiple customers on a single network, or be a network dedicated to a single customer.

Private VPNs, firewalls, and other edge network security measures were not effective in preventing cyber criminals from getting into corporate networks

TAG Cyber: Given the current social and political climate, are you seeing new trends in attack methods, and new requirements from enterprise clients?

TELOS: There are a number of world events bringing about opportunities for cyber criminals to use attack methods that have significantly evolved in recent years: The impact of emerging technologies such as AI, 5G, quantum computing, and the internet of things (IoT). The impact of moving enterprise networks to the cloud, which compels organizations to be diligent in their understanding of the cloud's shared responsibility model and do their part to ensure compliance with security practices. Other global events such as the role cyber security will play in the U.S. presidential election; new fronts in cyberwarfare; increasingly targeted and profitable ransomware attacks; the ongoing issues of personal data privacy and the best way to deal with identity and authentication. There are increasingly effective types of cyber attacks on new targets and ongoing organizational restructuring to address the issue of cyber defense and what do about the cyber security skills shortage.

TAG Cyber: That's a long list of things making the digital realm more complex and potentially dangerous! If someone wants to stay totally anonymous, couldn't cyber criminals or, on the other side, law enforcement, just watch the exit nodes?

TELOS: Anyone with the right tools can monitor internet traffic. That is, specifically, why Telos Ghost was developed—to assure total privacy and elimination of attack vectors while using the internet. Telos Ghost ensures that anyone watching traffic at an exit node cannot track that traffic back to the source. The user and their organization are protected from anyone being able to determine their identity or their location.

Further, through managed attribution, users can change the exit node they are using at any time. Users can swap IP addresses of their exit node at any time. Users can remote their browser to a virtual session and modify the attributes of their browser to create the persona they wish to be seen on the internet, further masking their identity and location. For users who must have total private connectivity between end user devices and corporate enterprise networks, the exit node can be located in the private network enclave, either at an on-premises location or a cloud location. These capabilities ensure that the user can select the level of attribution needed for their specific objective and ensure no activity can be tracked back to them or their organization.

TAG Cyber: What are potential legal, compliance, or regulatory considerations for enterprises using cloaking in different regions around the world?

TELOS: We believe Telos Ghost enhances the ability to ensure the levels of privacy for which regulations such as the General Data Privacy Regulation in the EU and the California Consumer Privacy Act were developed. With Telos Ghost, the protection of a user's data, identity, and location are hidden from cyber criminals, eliminating attack vectors to ensure private data stays private.

AN INTERVIEW WITH WITH RYAN TROST, CO-FOUNDER AND CTO, THREATQUOTIENT

FINDING THE RIGHT DATA TO ASSESS BUSINESS THREATS

Security operations center (SOC) teams are overwhelmed by the amount and pace of threats in the cyber security landscape. Today's organizations are more digitally complex than ever, and adversaries can be lurking in any corner of the globe and have any manner of motivation to attack. In some cases, cyber attacks are opportunistic. In others, they're targeted, based on what type of intellectual property a company has, who its executives or partners are, political or social beliefs, the size of its customer base, the amount of financial data likely collected and processed, and more. Add to that the countless ways an organization could be exploited—phishing, unpatched systems, flawed code, and so on—and it's easy to feel like defending against attacks is impossible, let alone having the ability to take a proactive approach.

Cyber threat intelligence emerged as a formal discipline nearly a decade ago. Since that time, what started as data feeds and alerts has turned into a much more robust area of technologies and techniques for identifying and handling threats. Ryan Trost, Co-Founder and CTO of ThreatQuotient, has been on the front lines of threat intelligence since the beginning. We talked to him about what threat intelligence means today.

TAG Cyber: How has threat intelligence as a domain evolved over the last decade?

THREATQUOTIENT: Threat intelligence has evolved significantly over the past decade—beginning in the initial traditional hype cycle with more conceptual innovation, to today where it is in the industry limelight and delivering operational bite. Today, teams are implementing intelligence programs within their SecOps workflows and are aligned to their technologies, budgets, and resources.

TAG Cyber: You've talked about the importance of getting the "right data." Can you explain what that means?

THREATQUOTIENT: In the context of threat intelligence, "right data" means accurate, timely, and actionable and encompasses both internal data and external data. Internal data includes metadata-rich network and application log and alert data but also extends to organizational points of contact (outside the immediate security department) to help efficiently navigate investigations.

TAG Cyber: We hear about "context" a lot, but what does it actually mean in relation to threat intelligence, and how does it impact security operations' teams decision making.

THREATQUOTIENT: "Context" is the supplemental information that helps describe a piece of information—typically in the form of an indicator of compromise or indicator of attack. For instance, a single IP address or FQDN is pretty useless unless it is accompanied by additional context including timeframe, target industry, attack vector, adversary leveraging it, or even source of that intelligence. Most SecOps teams

…that person needs to be a senior, well-seasoned analyst who can identify suspicious activity within an organization.

won't take action on intelligence passed to them unless it is accompanied by additional context because that additional context—supporting information—allows them to truly assess the threat to the business.

TAG Cyber: When, how, and who should implement a threat hunting program?

THREATQUOTIENT: Threat hunting is an ambiguous term which means a lot of different things to different people. However, in my operational experience, threat hunting is the process to discover, pursue, and mitigate an adversarial foothold within the organization without the initial trigger of a SIEM alert or notification. Most security teams have probably incorporated smaller threat hunting programs across their security analysts and incident responders to help minimize "SIEM burnout." However, implementing a dedicated threat hunting program can be a tricky process because in order to see a return on investment in the role, that person needs to be a senior, well-seasoned analyst who can identify suspicious activity within an organization. These types of resources can be hard to find.

TAG Cyber: Can you tell us a little about ThreatQ Investigations?

THREATQUOTIENT: ThreatQ Investigations is the industry's first cyber security situation room designed for collaborative threat analysis, shared understanding, and coordinated response. ThreatQ Investigations allows real-time visualization of an investigation as it unfolds within a shared environment, enabling teams to better understand and anticipate threats, as well as coordinate a response. The solution, built on top of the ThreatQ threat intelligence platform, brings order to the chaos of security operations that occurs when teams work in silos, acting independently, inefficiently, and unable to share intelligence and tasks easily. ThreatQ Investigations answers this industry challenge by providing a single visual representation of the complete situation at hand, including what actions were taken, by whom, and when.

AN INTERVIEW WITH WITH STEVE PRESTON, SENIOR VICE PRESIDENT OF STRATEGY AND GROWTH, TRAPX

RAPID TIME TO VALUE WHILE DECEIVING CYBER ADVERSARIES

On every security practitioner's wish list is the ability to anticipate then block attacks against their employer's network, helping avoid costly, damaging cyber incidents. While most security vendor technologies aim to meet this need, there is perhaps no better method of foiling one's adversary than through deception. Deception technology has been part of the cyber security toolbox for many years, but recently, a new breed of companies has started to focus on the lifecycle of an attack. That is, the goal isn't simply diverting threats to a decoy, but providing users the ability to disable and neutralize attacks then automate incident response playbooks.

Recently, we spoke with Steve Preston, Senior Vice President of Strategy and Growth at TrapX, one of the leading providers of deception technology, about the evolution of advanced attacks and how the threat landscape is changing. In the face of work from home and the fear, uncertainty, and doubt that accompanies our current social and political climate, cyber criminals are cashing in. TrapX has opinions on how to right the balance in favor of defenders.

TAG Cyber: Given the current state of how employees must work, it would seem the endpoint is the starting place for hardened controls. What's your viewpoint on endpoint security?

TRAPX: Hardened or not, endpoints are connected to the internet via home routers and in turn connected to other home computers and devices which are likely vulnerable so where does it end? And let's not forget the users, they are certainly vulnerable! But, let's think about attacker goals. Are those goals to control an endpoint or exploit it to gain control of critical asset? It's the latter, of course! The endpoint is only the vehicle that gets attackers to their goal.

We should harden endpoints, but as the saying goes, "the attacker only has to be right once," so we should also assume that an employee can and will be compromised at the endpoint (the industry has more than enough data to prove this to be true) and add an internal security layer that channels the would-be attacker away from critical assets, all the while, making them think they are hitting the jackpot.

TAG Cyber: What are some of the challenges with traditional or legacy deception technology?

TRAPX: Honey pots have been around for a while and the have earned a reputation for being complex. In fairness, the original design objective for honey pots was to learn, and to that end, they work as designed. But we've found that some commercial deception tools are essentially modern honey pots; they allow attackers to interact indefinitely. They deliver value but they're still built to learn and they can take several

we've found that some commercial deception tools are essentially modern honey pots; they allow attackers to interact indefinitely.

months to implement so their scalability and flexibility is limited. On the other hand, there are tools that are based on lures—artifacts like fake credentials, files, or browser history—on the endpoint designed to deceive. These products don't deliver deep insight, but they're valuable and they scale well, provided you can get past the objection of lightweight lures existing on the endpoint (a non-starter particularly for IoT or OT). So given these choices, a CISO would either use both or make some trade-offs: Learn or deceive? Insight or scale?

TAG Cyber: How is TrapX different?

TRAPX: TrapX was designed to detect and respond to attacks, not just catch and learn. This required an agile platform that can deploy, scale, and adjust quickly while providing enough insight to expose an attacker's TTPs, and then respond to the attack. We achieve this with emulated traps. This is patented technology that's fundamentally different. Emulated traps are identical to real assets and just deep enough to engage an attacker long enough to generate high fidelity alerts. This architecture scales—500 traps in just minutes, and that gives our customers an agile platform which deploys and adjusts quickly while delivering immediate time to value. Another benefit is that our emulated traps don't touch assets and that makes it a perfect fit for both IT and OT environments.

TAG Cyber: What kind of internal team is needed to support use of your product?

TRAPX: One of our customers told us we helped him build a Ferrari with a Volkswagen budget. TrapX stands up quickly and is really easy to use. Anyone in IT or security who wears an analyst hat full or part time is able to use it. I should mention that TrapX is not a noisy tool. When it's configured properly, it doesn't generate false positives. Our customers tell us that their alert volume goes way down with TrapX in the environment.

TAG Cyber: You recently released a cloud deployment option. Outside of the obvious, is there an added benefit?

TRAPX: Right, some of our customers want TrapX in the cloud as a deployment option but there's more to it, of course. Our cloud offering means that we can now provide an anonymized pool of active attacker TTPs that our customers can learn from. It's a centralized repository of sorts; enterprises can detect threats in their own network but now also see what's happening among their peers and plan accordingly. That's really valuable and it has huge potential for defenders.

AN INTERVIEW WITH WITH CHAD BOECKMANN, FOUNDER & CEO, TRUSTMAPP

UNDERSTANDING SECURITY PERFORMANCE MANAGEMENT

Enterprise security assessments represent one of the most common activities for modern business and government teams. Such assessments focus on identifying levels of cyber risk, and the goal is generally to optimize the investment being made in cyber security controls. A number of good frameworks exist to provide guidance for these assessments, including the familiar NIST Cybersecurity Framework (CSF) and the Payment Card Industry (PCI) Data Security Standard (DSS).

The challenge with assessments is that they represent so-called point-in-time reviews. To establish an ongoing view, enterprise teams are beginning to focus on a new assessment method known as security performance management (SPM). SPM engagements are continuous and include findings based on repeating cycles of assessment, reporting, modeling, and remediating. It is possible that SPM might represent the future of enterprise security assessment, consulting, and audit.

The TAG Cyber team recently sat down with Chad Boeckmann, Founder & CEO of TrustMAPP. The company has pioneered platform solutions supporting the SPM approach and we were interested to learn more about how this was working in the enterprise marketplace.

TAG Cyber: What are the main problems that arise with point-in-time assessments?

TRUSTMAPP: We believe that there are five main challenges security teams face with point-in-time assessments, and TrustMAPP helps with all five. The first is consistent security messaging—making sure that security has consistent, repeatable metrics, KPIs, and KRIs. When every assessment is treated as a one-off, it's easy for the metrics to change every time and you lose the consistent view that is needed to conduct a proper evaluation of trending maturity and risk.

The second challenge is what we call business narrative. That is, the ability of the CISO and their team to effectively communicate the organization's security posture to every stakeholder: C-suite, Board of Directors, compliance teams, risk management teams, and SecOps. Currently, most assessments are written by auditors for CISOs and are filled with jargon that is compliance-oriented and does not speak to the organization's business goals and objectives: What is our financial exposure, and what will it cost to remediate that exposure—in time and dollars—and how does investing in Y achieve X?

The third challenge is trend information. Point-in-time assessments might let you check off another to-do item, but they do not let you run cyber security like a function of the business. Every other department is expected to show progress, trends, over time, and boards now want to see the same progress and trend reporting in the security program, and be able to compare the company's security maturity and progress to peers.

A lot of organizations have never asked themselves, "What is our risk appetite?" And if you never ask, then you never answer. But it's crucial to understand, or else you will not clearly know if you are spending the "right" amount of resources on cyber security. You will inevitably end up spending too much or too little on security based on your assumptions. Instead, you should base decisions on the organization's known objectives and the variables within your individual business that affect the ability of the cyber security program to achieve those objectives.

Finally, most assessments today don't give the senior leadership the information they need to prioritize investments in people, process, and technology: What will it cost? How much will it reduce your risk? What project needs come next and which can wait for a later budget cycle? These are all questions that must be answered.

TAG Cyber: Do these problems invalidate the types of assessments and audits that enterprise teams might have done in the past?

TRUSTMAPP: No, I wouldn't say that these issues invalidate the past approach—the traditional GRC approach was the best that was available at the time. But, as with anything else, things evolve, get better, faster, easier. That's what SPM represents, an evolution of maturity assessments. GRC was a good idea—it was better than plain old spreadsheets. But it still approaches assessments as point-in-time engagements, with minimal trending, and no real-time visibility into ongoing improvements. Most importantly, it doesn't tell you what to do next and quantify the improvement to near real-time posture scores. With SPM, we're bringing a continuous process approach, which allows continuous accountability and transparency, and we can recommend next steps, with associated costs, while tracking those improvements across multiple stakeholders.

most assessments today don't give the senior leadership the information they need to prioritize investments in people, process, and technology

TAG Cyber: Tell us about this concept of SPM. How does this work?

TRUSTMAPP: SPM is really all about treating information security like any other part of a business. It has to be accountable, it has to be measurable and quantifiable, and it needs to always get better. SPM is meant to leverage existing investments in people, tools, and processes; integrate all the information; and create intelligent, automated workflows. SPM is also really focused on communication, so CISOs can present information to a variety of stakeholders in language that makes sense to those stakeholders, not just security profesisonal, ultimately delivering business intelligence.

TAG Cyber: How does SPM rely on and use automation?

TRUSTMAPP: In the people-process-technology triad, traditional assessments relied on lots of people time and manual processes.

GRC solutions attempted to introduce some technology to that, to unburden people somewhat. But the processes remained largely manual. With SPM, we are really raising the bar on the technology in order to automate the processes of measuring, communicating, and managing. To give just one example, in our SPM platform, the proctor can assign assessment questions to various respondents on the team. The platform automatically emails those people, tracks their responses, and lets the proctor know that there are responses to be validated. And the status of all the in-flight activity is visible in real time in the SPM security dashboard.

TAG Cyber: Do you expect consultants, assessors, auditors, and regulators to adopt the approach?

TRUSTMAPP: Yes, and we're already seeing it with some of our early customers and solution partners who run cyber risk practices. Cyber posture assessments have always included people, process, and technology. SPM doesn't change that, but it raises the bar by increasing efficiency and creating a unique engagement approach, making assessments faster and more impactful, with real-time updates on progress and performance—turning raw data into business intelligence. Our partners instantly see the difference this approach creates because it elevates the engagement and naturally creates a more strategic conversation.

TAG Cyber: Any final thoughts on the future of security performance management in our industry?

TRUSTMAPP: All of our company's metrics are moving up and to the right, and I think that's true for the whole product category. It's still a relatively new category, so there is a lot of opportunity globally. Once organizations discover that they can have meaningful decision support, on-demand, while tracking performance to budgets and risk outcomes (which is basically what SPM is), the value proposition quickly becomes obvious.

AN INTERVIEW WITH WITH SAMEER MALHOTRA, CEO, TRUEFORT

PROTECTING THE ENTERPRISE APPLICATION ECOSYSTEM

Businesses today describe their mission in terms of their applications—and this implies that securing their application environment has emerged as one of the most consequential aspects of modern organizational protection. The good news is that many excellent solutions are available to reduce application security risk, but the challenge is selecting and orchestrating the best approaches.

Recently, it's become clear that applications are increasingly a target-rich threat to business continuity, often from nation-state actors, and require special focus on detecting and responding to both existing (known) and yet to be discovered (unknown) exploits. As a result, an emergent category known as application detection and response (ADR) has become an important consideration for security teams and enterprise chief information security officers.

We recently spent time with Sameer Malhotra of New Jersey-based TrueFort to discuss his team's pioneering work in the area of ADR. TrueFort has been securing enterprise-wide application environments for many years using its differentiated approach to collecting telemetry from running applications, behaviorally profiling these running applications, and using the resulting insights to accelerate and guide optimal security response.

TAG Cyber: You've been an expert in application security for many years, including considerable time as a practitioner in financial services. How has application security evolved over the years?

TRUEFORT: When I first started, and even through my later experiences as a security executive, much of the industry's entire approach to security has been what I call infrastructure-centric. We'd deploy a vast number of security tools to protect our IT infrastructure: firewalls, host-systems, vulnerability scans, malware detection, and filtering, etc. All important stuff.

But my big insight came when I experienced a massive breach at my employer at the time, a very large and well-known investment bank. The immediate request from the CISO was to present a business impact report, i.e., he needed to communicate with the rest of the company about how and where this breach might compromise the overall company operations. And those operations were run on applications. However, most of our security systems and tools were infrastructure-centric so they could only report on potential compromise of a specific host or firewall, but there was no up-to-date operational visibility into the context of how those distributed systems rolled up into specific applications. Our applications were a connected web of interacting components across multiple systems.

It took us weeks of time—using sometimes out-of-date spreadsheets—from a large chunk of our security team to assess the risk

impact through a lens that the business team could understand. The business would ask, "was this critical application and its data affected?" We couldn't easily answer that question despite having a very large security budget.

Everything changed after that. So, security of applications, and the entire application environment itself, has been evolving towards empowering security teams with better visibility, controls, and response capabilities so they can not only more effectively protect applications, but also give a real-time view into the business risk associated with potential application risks.

TAG Cyber: Tell us about your platform. How does it work?

TRUEFORT: Truefort was purpose built to give security teams a robust way to protect their entire application ecosystem. We do that by tapping into the existing security telemetry most enterprises are already generating from existing agents such as EDR (Crowdstrike, for example). But we can also use other existing security data sources like data lakes. The key is that we continuously collect, ingest, and present relevant critical telemetry through what we call an application context. This means that we provide operational security visibility into the entire application ecosystem such that our customers can identify and respond to both known and unknown threats and hidden risks in real-time with the knowledge of how those application threats and risks might negatively impact their business if not addressed.

In addition to providing this visibility, we also layer on a comprehensive suite of security controls focused on securing application and cloud workloads. So critical elements of cloud workload protection such as network segmentation, system integrity assurance, application behavior whitelisting, memory protection, and integrity monitoring are all provided by Truefort into a single solution platform that we refer to as full stack cloud workload protection. Our customers refer to the value of our approach as giving them a more effective way to manage their overall application risk posture across an entire application portfolio, whether hosted in their data center or via private, hybrid, or public cloud.

there was no up-to-date operational visibility into the context of how those distributed systems rolled up into specific applications.

TAG Cyber: What is new about ADR? Does it focus more on dealing with attacks and exploits that cannot be prevented?

TRUEFORT: We see ADR as more of an application-centric component of an overall strategy to make security operations teams more responsive and proactive in identifying potential threats and reducing response times. There's an emergent trend called XDR that is really focused on better data aggregation and correlation across disparate security tooling to improve SOC

effectiveness. We see ADR as a component of that strategy but focused around application-centric data visibility and security controls optimized for protecting applications and accelerating incident response when applications are impacted.

Truefort does two things better than any other solution in the market in this regard. First, we help security teams quickly and easily see hidden security issues related to applications and how those applications interact with each other. Most enterprises we talk to have no idea how their application ecosystem is interacting, it's just too complex and dynamic, which makes the security team's job very hard as they are deluged with disconnected data that might or might not be relevant to securing their applications. Second, and this is critical, we behaviorally profile running applications to determine what is "normal," i.e., secure, operationally. We then allow security teams to auto-generate compliance policies such that any anomalous behaviors are surfaced immediately, and teams are alerted to the change. So, a low and slow attack, for example, where a bad actor has penetrated the perimeter in an attempt to quietly exfiltrate data, will be detected by us in real time because it will trigger anomalous data use behaviors related to specific applications.

TAG Cyber: What is the impact of CI/CD on application security? How does your platform integrate into these Agile environments?

TRUEFORT: This is a great question because at the end of the day you'll have much better security if you can avoid pushing application security risks into your production environment in the first place. We impact CI/CD by giving application development and DevSecOps teams a way to add security compliance testing into their existing toolchain for running automated functional tests. Security compliance becomes just another testing component that an application update or module must pass before it is deployed into production. DevSecOps can set up policies governing acceptable application security behaviors and those policies can then be used to automate compliance testing as part of the overall build and test chain. Deviations from policy are detected and the developer is alerted to the problem as they would any other functional test failure. This gives the developer the chance to modify any relevant security-related code elements to bring them into compliance before the final push to production.

TAG Cyber: What do you see on the horizon for protecting application ecosystems and also ADR?

TRUEFORT: The biggest request we see from CISOs and their security organizations is to help them translate complex security

operational status and practices into a cogent distillation of risk impact to their business. Security teams can be much more effective if they have understanding of how to prioritize in alignment with what's best for the business. If one of their top critical business applications is showing anomalous behavior indicating potential compromise, then teams want to know that in real time so they can prioritize response over other security issues that might be important but not business-critical in that moment.

So, to your question, what we see on the near-term horizon is giving CISOs (and their teams) a comprehensive real-time view into their enterprise's overall application ecosystem risk posture such that teams can easily prioritize their activities aligned to the business impact and outcomes. Because ultimately that is what this is all about—making the security team a more effective protector of the assets of the business. And applications, along with their data, are right up there on the top of the list as some of the most critical business assets requiring protection.

AN INTERVIEW WITH WITH KEITH STEWART, SVP OF PRODUCT AND STRATEGY, VARMOUR

DYNAMIC AND CONSISTENT VISIBILITY THROUGH APPLICATION RELATIONSHIP MANAGEMENT

Today's highly complex, hybrid, and application-dominated networking environments place a new level of onus on security and operations (SecOps) teams. Whereas in the past, SecOps needed to know which endpoint was talking to which server, today, environments and apps can spin up and down instantly, change overnight, and disappear tomorrow. Keeping track of what on and what's communicating on your networks has become a tangled and dynamic mess.

This is why over the last several years the commercial security market has seen an explosion of technologies that promise full visibility into your networks, whether they're on-premises, virtual, in the cloud, software-defined, or hybrid. And buzzworthy though it may be, there is truth in the fact that you cannot manage that which you cannot see. This is the premise behind vArmour, an application relationship management company that focuses on native APIs as the basis for understanding, simplifying, and controlling the applications on your network. We recently spoke with Keith Stewart, SVP of Product and Strategy, at vArmour about the company's evolution into application relationship management.

TAG Cyber: Let's start with the basics: What is application relationship management? It's a term we are hearing more often around the industry.

VARMOUR: Customers need a modern security approach that can keep up with the pace of digital transformation. With factors like the global pandemic, that pace is accelerating and creating a difficult challenge for enterprises to secure both their new and old infrastructure. For example, if I have Azure, AWS, and a data center, there could be hundreds of thousands of dynamic relationships between workloads and applications within and across these environments. How do I know which relationships are the risky ones? Where are my critical assets and are they at risk? You need an approach like application relationship management to solve these problems.

Application relationship management enables enterprises to understand real application behaviors so that policies can be developed to reduce exposed attack surfaces while not impacting the operation of the application. By capturing real-world application communication patterns across multiple environments and infrastructures, an application relationship management solution discovers workload types, application clusters, and dependencies so that security administrators can visualize application relationships and create granular intent-based policies to keep applications secure. Relationship maps enable IT to classify applications, and/or enrich their sources of truth such as configuration management databases (CMDBs).

A relationship-centric approach observing actual behaviors between workloads and applications is needed if you are seeking to achieve a source of truth for your dynamic enterprise.

The collected data also accelerates reporting and investigative tasks for compliance monitoring, network troubleshooting, and incident response.

TAG Cyber: Why focus on relationship management versus event management, which is more common?

VARMOUR: Cloud is forcing the transition to relationships, and for two reasons. The first one is that the cloud has caused a fragmentation of applications, along with the environments they run on. As a result, you have an explosion in the number of relationships that need to be understood and secured. The second reason for focusing on relationships is that the cloud is dynamic with a high speed of change. Static systems like CMDBs require highly manual configuration, and as a result, become quickly outdated. A relationship-centric approach observing actual behaviors between workloads and applications is needed if you are seeking to achieve a source of truth for your dynamic enterprise.

Event management has been the basis of classic IT and security operations, but it lacks the context of applications, despite organizations spending millions to process billions of events per day. On the other hand, relationship management can enable ops teams to clearly see dependencies and risks across their application portfolio. It can provide visibility of the microscopic relationships between individual workloads, but even more importantly, the macroscopic relationships across business units and clouds to truly assess the risk of the enterprise.

TAG Cyber: What are the primary use cases for vArmour?

VARMOUR: The primary use cases for vArmour fall into three buckets. The first one is reducing operational risk for the enterprise. This is where vArmour provides dynamic and consistent visibility of application relationships across both new world and legacy systems to visualize and control application dependencies and incident impact. The second use case is increasing application resiliency. This is where we can isolate and protect critical business applications with automated, environment-independent policy governance and orchestration. The third use case is for accelerating cloud adoption. We solve the "policy problem" that often prevents application migration by automatically applying consistent policies pre- and post-migration.

TAG Cyber: What types of telemetry can admins/operators expect to get when they deploy vArmour?

VARMOUR: Let's first talk about how vArmour is deployed. Only vArmour lets enterprises get more value out of the investments they've already made. Installing new agents or infrastructure is

time intensive and costly. Yet the technology enterprises already own have all the data and controls they need—from APIs and flow logs to security groups and distributed firewalls. vArmour provides enterprises with end-to-end visibility and control by leveraging the power of their existing platforms—whether it's VMware NSX, AWS, Microsoft Azure, Cisco ACI, Tanium, or other platforms.

From these platforms, vArmour ingests all kinds of telemetry—things like cloud, network, agent, SDN, middleware—to model applications and identify interdependencies, and enriches this information with things like CMDBs from ServiceNow or BMC, or GRC info from RSA Archer. This information is stored and analyzed within the vArmour's Relationship Graph, allowing a common view of complex, interdependent systems. The Relationship Graph is continuously maintained to ensure that material changes to application behavior or interdependencies can be immediately identified.

AN INTERVIEW WITH WITH DIDIER LESTEVEN, COO, WALLIX

SECURING ACCESS TO ACHIEVE DIGITAL TRANSFORMATION

Account over provisioning has been a leading cause in numerous security compromises over the years. Companies need to reign in the access users, systems, and processes are granted, all without inhibiting access for legitimate use. Privileged account management (PAM) seems to be the easy answer, yet many organizations deprioritize PAM given organizational constraints and difficulty of use; ephemeral environments, rapid software development/deployment, and ever-changing users and user roles are difficult to track, thus increasing complexity and requiring administrators to (often) manually adjust policies and permissions continuously.

Nevertheless, security and operations teams must employ strict access controls that allow users to do their jobs and systems to run as intended without exposing the organization to unnecessary vulnerabilities. WALLIX is a software company offering zero trust privileged account governance, including PAM, identity-as-a-service, session monitoring, and remote access management. We spoke with Didier Lesteven, COO of WALLIX, about today's access control and identity management challenges.

TAG Cyber: Workforces are operating more remotely than ever before, and resources are largely decentralized. How is this paradigm impacting how companies secure access?

WALLIX: As more and more individuals and teams make the switch to remote work—either temporarily or indefinitely—security becomes a major concern. Each employee who takes their laptop outside the corporate network perimeter or connects into IT resources from an external location creates new vulnerabilities. The main issues with remote access security are knowing 1) who is accessing your systems, 2) which resources they have the rights to access, and 3) what they are doing with that access.

Ultimately, securing access is paramount. This massive shift towards decentralized workforces and external access is forcing IT teams to find solutions as quickly as possible for their colleagues to do their jobs securely with as little disruption as possible.

One of the most efficient ways to achieve access security quickly and efficiently is with privileged access management. The right PAM solution offers complete control over privileged users, granting and revoking privileges to access IT resources as and when they're needed. With integrated PEDM (privileged elevation and delegation management), organizations can implement a least privilege approach to further secure remote access, enabling them to temporarily elevate and delegate privileges.

This can be taken even further with an endpoint privilege management (EPM) solution, which ensures that privileged access is limited and

controlled at a granular level—eliminating endpoint administrator rights—for endpoints both inside and external to the corporate network without impacting the user's productivity.

A robust PAM-PEDM solution offers a suite of powerful capabilities that help organizations protect their most critical IT infrastructure, no matter where it's being accessed from. It secures remote access of employees or third-party contractors and allows precise control over their access—which resource, which application, which commands or actions, and when/for how long. Furthermore, users accessing these resources never need to know root passwords, which avoids the lost or stolen credentials that present such a significant security risk. Comprehensive session management means businesses can not only grant privileges, but have full oversight of privileged users' work, including OCR recording of all keystrokes and clicks, enabling shared sessions, and facilitating automated session termination when necessary.

Ultimately, the aim of PAM is to simplify security and productivity. It streamlines privileged user management for IT teams, makes it easy for users to request privileges when needed, and has no disruptive impact on user workflows, keeping businesses productive and efficient.

TAG Cyber: The CCPA in the U.S. recently passed its enforcement date. How do regulations like CCPA, GDPR, and other compliance regulations change how organizations need to think about access?

WALLIX: At their core, GDPR and CCPA are quite similar, requiring companies to regulate who has access to data, what access they have, when they have it, etc. And, significantly, they apply to any company with customers in the relevant territory—whether or not the business is located there. Thus, organizations need to ensure that their systems and technologies adhere to the minimum standards of these regulations (and those sure to come in the future) to achieve compliance.

The key is to think of data protection as more than simply locking a box. Who has access to it? When? How is their access and use of the data being traced? Securing data requires securing privileged access. And with GDPR now well established and CCPR in full force, companies who are late to the game need to find a solution that not only answers these security needs, but one that is easy to implement and manage to become compliant as quickly as possible.

PAM technology with an agentless architecture can simplify the task for IT, offering quick deployment and easy maintenance. One lesson learned from the roll-out of GDPR is that any tool that is overly complex or unduly burdens a user will be avoided and

The right PAM solution offers complete control over privileged users, granting and revoking privileges to access IT resources as and when they're needed.

therefore hinder compliance—risking major fines and possible data breach. IT administrators need to be able to set the rules of access permissions and enforce policies on privacy for administrators and employees worldwide. A single console that manages access to all data resources facilitates compliance. Strong access management functions to define and enforce a single point of privileged access, a password vault feature that secures and rotates login credentials, and a session management function that generates detailed reports are all critical.

TAG Cyber: You emphasize ease of use with WALLIX Bastion, your flagship product; how is the Bastion different from traditional PAM solutions?

WALLIX: The WALLIX Bastion solution suite (including our access manager) is the only PAM-PEDM solution delivered as an appliance, meaning that it embeds its own global operating system (kernel, database, file systems, etc.). There's no need to think about how many Windows server licenses you have to deploy and maintain, nor databases and orchestration of file systems. This facilitates rapid and easy deployment, while delivering a highly complex security solution and yielding the best TCO of any comparable solution in the market today.

The WALLIX Bastion is highly intuitive with a modern and simplified GUI. Our solution is mainly proxy-based, eliminating the need deploy and manage complex agents on servers or applications.

In addition, the WALLIX Bastion offers an open and documented API interface which enables broad interoperability with other security solutions such as IAM, SIEM, MFA, etc. or applications for enhanced cyber security.

TAG Cyber: How is securing access in industrial, IoT, and critical infrastructure different from traditional networks?

WALLIX: As manufacturing groups move into an era of hyper-connectivity, industrial control systems (ICS) have begun interacting with equipment in more nuanced ways: Information Technology (IT) and Operational Technology (OT) are converging. Today, data from the factory floor can be monitored and analyzed in real time to assess efficiency and productivity. These reports can then be relayed back to the equipment within seconds with instructions on how to improve.

This interconnectivity, while transformative in terms of business opportunity, is also rife with cyber security risk. Historically siloed ICS are suddenly connected to IT and, thus, exposed to the internet. These systems are heterogenous, mixing new and old technology, much of it predating the existence of IoT, and are the sort of cyber security risks which 21st century businesses are growing to expect. This wide variety of technology also

presents certain challenges when trying to apply modern security solutions which may not be adapted to older operating systems.

Beyond the challenges of legacy technology, an industrial context also brings with it the risks of health and human safety. Unlike a financial or commercial organization, security threats to industry can put lives at risk. Malicious hijacking of ICS could result in widespread blackout of public utilities or endangering the workforce with a loss of control over industrial equipment.

The solution, then, is to reintroduce an airgap between IT and OT, this time in the form of access security. Smart factories can continue to grow into the digital transformation, with the help of privileged access management solutions that control who has permission to access which critical equipment, when they can access it, and what they are permitted to do. Complete, precise control over permissions with additional layers of identity management and session monitoring (and automated termination) facilitates modern security in complex IT-OT-IoT environments.

TAG Cyber: How can better authorization and authentication actually accelerate digital transformation?

WALLIX: Digital transformation implies that everything is becoming connected and accessible by digital means. This also means the attack surface is growing to match. It is imperative to know, at all times, who is accessing what in your IT infrastructure, and this can be done through the implementation of security solutions across the entire IT/OT system. To accelerate digital transformation you must:

- Identify "who" through identity management
- Authenticate that the identity is who/what they claim to be, preferably through multi-factor authentication (MFA)
- Authorize by granting and revoking rights according to need

Digital transformation is full of opportunity for businesses to move quickly, but cloud services and digital technologies create new vulnerabilities. Implementing well-chosen security solutions which offer robust protections and encourage productivity can enhance and accelerate digital transformation. Security solutions such as PAM, IdaaS, MFA, and EPM help ensure that critical assets are protected, monitoring and tracing access and activity across the entire digital workplace, and blocking vulnerabilities with ease. Organizations can move quickly and stay agile in a constantly evolving business world when they are confident in their security posture.

AN INTERVIEW WITH WITH ANDREW GINTER, VP INDUSTRIAL SECURITY, WATERFALL

CONTROL THE FLOW OF INFORMATION. CONTROL CYBER ATTACKS

When we think of OT, we think of critical infrastructure (CI): power generation, rail systems, oil and gas, manufacturing, and utilities—industries which ensure the physical health and safety of our society. While digital transformation has placed requirements for constant uptime and availability on CI and non-CI networks alike, the consequences of an attack against enterprise networks are generally not life-threatening.

Yet, as industrial operations have become increasingly automated, IT and OT networks have converged as a matter of convenience, and thus security operations teams have adapted cyber security technology designed for IT networks to run on OT networks. However, given the scale of consequences of compromise for OT networks, operators are learning that traditional IT security controls are not always sufficient for industrial control system (ICS) environments. Waterfall Security isn't just adapting IT security for use in ICS environments; the company's unidirectional gateways are adding an entire layer of protection for ICS networks in addition to conventional IT security technologies. We spoke with Andrew Ginter, VP Industrial Security, about ICS security and how Waterfall is serving CI customers.

TAG Cyber: It seems obvious in hindsight to use unidirectional gateways on critical systems. But how did Waterfall Security come up with the concept, and why?

WATERFALL: Waterfall was founded in 2007, and the technology was already a gleam in our founders' eyes in 2004. Back then, the concept of unidirectional communications was in regular use in government and military networks for decades already. What was new was the imperative to protect industrial networks. It was roughly 2004-2007 when sophisticated, targeted nation-state attacks were starting to show up on the radar of a lot of organizations. These are the attacks that pioneered the attack techniques that are now commonplace for industrial espionage, targeted ransomware, and even some hacktivist-type attacks. Israeli authorities were concerned about this development and ordered that the nation's critical infrastructures be protected against such attacks.

Our founders stepped up to look at the problem. They observed that while the ICS networks of the day sent a fair bit of information out to enterprise networks, ICS networks needed almost nothing to come back. And so they experimented with replacing IT/OT firewalls with unidirectional hardware—hardware that was physically able to send information in only one direction. They quickly discovered that the key to deploying such protection was the software. So they invented the concept of a unidirectional gateway: a combination of unidirectional hardware with special industrial software. Unidirectional gateway software is not a router, like a firewall—the software does not forward network packets. Instead, unidirectional gateway software

synchronizes databases and other systems in one direction only. Enterprise users and applications can then access replicas of industrial databases and industrial data sources without changing any access technologies or procedures. The software makes the unidirectional hardware invisible to the enterprise. And thus a business was born.

TAG Cyber: Why not simply air gap OT networks?

WATERFALL: Well this was 2004-2007. As early as the mid 1990s, industrial enterprises had already started connecting IT and OT networks so that they could get online access to industrial data. This was because they had figured out how to profit from the data. For example, one of the early drivers was predictive maintenance. The numbers showed that large industrial sites could save 3-7% of total operating costs by tracking how long and how hard each piece of equipment had been used, and delaying maintenance work until it was needed rather than schedule maintenance every 2-3 months whether it was needed or not.

Now, 3-7% might not sound like a lot of money to some people, but these are massive operations. And a lot of these businesses produced commodity outputs—gasoline, electricity, etc. As a result, the businesses generally operate with razor-thin profit margins. Three to seven percent might be the entire profit margin for the facility. Therefore, everybody was deploying these systems, which demanded that the enterprise resource planning (ERP) systems could see every piece of equipment and how much it had been used, in real time. You can't do that with an air gap. In most industrial operations, air gaps were ancient history by the turn of the century.

TAG Cyber: How does the use of cloud in CI complicate OT network protection?

WATERFALL: We see cloud manifest in CI primarily in Industrial Internet of Things (IIoT) applications. This is where devices and systems that are used in industrial operations are connect straight out to cloud-based vendors. And again, perhaps not surprisingly, the first killer app in this space is predictive maintenance. The problem is security. The average manufacturing site has connections to 30-70 cloud-based vendors. The numbers are lower in power generation and pipelines, but they are growing rapidly.

A lot of people with a passing familiarity with the technology mistakenly assume that "unidirectional" rules out all remote support.

Are all of these cloud sites equally secure? Of course not. Some are more secure, and the occasional one is likely very insecure—and end users have no way to tell the difference. Compromise even one of these cloud vendors and now you are connected to hundreds of ICS networks at once and can drop ransomware or

whatever you want into all of those networks simultaneously. This is a disaster waiting to happen. This is why some CI sites are backing away from the space—simply forbidding such connectivity.

This is a problem, though, because forbidding ICS-to-cloud connections reduces efficiency and profits. There is compelling business value in these cloud connections. This is why Waterfall came out with our Unidirectional Cloud Connect (UCC) product a couple years ago. Again, almost all cloud connectivity pushes ICS data to the cloud, not vice-versa. UCC enables that data flow transparently and safely. It doesn't matter how many cloud vendors are compromised—nothing gets back into ICS networks to put continuous, correct, and efficient operations at risk.

TAG Cyber: If unidirectional gateways are implemented in OT networks, how does the user organization execute remote support, patching, continuous monitoring, and integration with third-party vendors/suppliers?

WATERFALL: Good question—this is a source of enormous confusion in the marketplace. A lot of people with a passing familiarity with the technology mistakenly assume that "unidirectional" rules out all remote support. In fact, Waterfall has a handful of remote support solutions in widespread use. The difference is that we produce and recommend the most specific solution to meet a support need.

Contrast this with firewalls for a second. "To a man with a hammer, all the world's a nail." To a man with a firewall? All the world's an open TCP port, preferably encrypted. You need anti-virus updates? Bang! Open a port. You need remote support? Bang! Bang! Open two ports, one for the VPN and one for remote desktop. You need OPC support (a popular industrial protocol). Whoa—that's DCOM-based. You're going to need a couple thousand ports open. Worse, we imagine that encryption makes our remote access "secure." In fact, cryptosystems encrypt attacks from compromised cloud and other endpoints just as happily as they encrypt legitimate communications.

What Waterfall recommends is the most secure, most specific solution to each remote access need—and given the priority for completely continuous and reliable operations, there aren't a lot of such needs. So we have server replication for continuous vendor monitoring. We have the FLIP—a temporarily-reversible unidirectional gateway—for anti-virus updates. We have Remote Screen View for receiving advice from third-party vendors. We have Secure Bypass for safe remote access for trusted insiders. Each of our solutions is the strongest currently available for a specific need, and we continue inventing new solutions as we see the threat environment and usage patterns evolve.

TAG Cyber: What data are you seeing about attacks on ICS that concern you most?

WATERFALL: Targeted ransomware is nasty and getting worse, but really, it's a symptom of a bigger trend. The attack techniques and technologies used in today's targeted ransomware attacks were the exclusive domain of nation-state-class adversaries only five or so years ago. Which suggests strongly that the tools and techniques of today's nation-state adversary will be pervasive threats in less than another half decade. Industrial sites really can't afford to redesign their networks and security every half decade.

Which is an opportunity for Waterfall. All cyber attacks are information, after all. This is what "cyber" means. Waterfall physically controls the flow of information with unidirectional hardware. Control the flow of information and we control the flow of cyber attacks, both current and future attacks.

AN INTERVIEW WITH WITH AHMED SHARAF OF XBAND ENTERPRISES

BENEFITS OF TAILORED SECURITY SOLUTIONS

From the perspective of any managed security provider, a major goal involves standardizing on the solutions being offered. Anyone who has had the pleasure to develop an income statement for commercial cyber security offerings understands this basic objective well: Repeatable, standard products provide scalable recurring revenue, and is thus a major aspect of the commercial solutions available to enterprise teams today.

But the fact remains that in many cases, tailored security offerings are coveted by enterprise teams. The customization that comes from personalized attention allows for tighter integration of a security solution into an enterprise, and for coverage of special cases that might include proprietary or non-standard controls. Consultants are helpful in this regard, but more often, an enterprise will turn to a security solution provider for such assistance.

We recently had the opportunity to connect with Ahmed Sharaf from XBAND Enterprises to learn more about how his team is developing and supporting tailored security solutions for enterprise. We wanted to better understand the trends in this area, and the types of functional, control, and support requirements that enterprise teams are requesting today.

TAG Cyber: Thanks for agreeing to share with us today, Ahmed. My first question is whether the security solution area can be viewed as sort of next-generation value added reselling (VAR) services?

XBAND: The pleasure is ours, and thank you for investing time with me and XBAND. No one provider can do it all, and while reselling is part of the equation, at XBAND we like to emphasize the "solution." Reselling typically has a beginning and an end. Historically the reseller magically re-appears at the end of the cycle. By having a continuous engineering solution mindset, we are able to proactively see and engage our clients in security discussions and help them adapt to mitigate the never-ending risks to the business.

TAG Cyber: Do you see the shift to cloud as having an impact in how enterprise teams work with security solution providers?

XBAND: Absolutely. Cloud is an important building block when it comes to security, and we would like to emphasize that business and enterprise security should be overarching and ubiquitous irrespective of the underlying cloud service provider or location. Shadow IT and scope creep are prevalent in the cloud, and therefore the business must have a strategy for how they will orchestrate and manage these resources.

TAG Cyber: What has been your experience with increased attention to work-from-home initiatives? I would guess that this requires focus in the solutions you offer?

XBAND: Given our historical origin in the internet service provider (ISP) space, we have extensive experience in remote access, work at home, and distributed solutions. Due to confidentiality, I cannot mention the employer or client, but nearly 15 years ago I lead the implementation of the

LET'S FACE IT, OFFICE365 IS OFFICE365 NO MATTER WHOM YOU ACQUIRE IT FROM.

first hosted contact center for a major global communication company and contact center outsourcer. For some, this is a little "Back-to-the-Future," with an element of business survival.

TAG Cyber: Do you generally combine professional, managed, and customized services in your solution offerings to enterprise? Is that a tough mix to manage?

XBAND: In short, we do, although what we have found is that many organizations lack standardization. As a general rule, up to 80% can be standardized delivering greater operating efficiency and financial benefits. Let's face it, Office365 is Office365 no matter whom you acquire it from. The remaining 20% is where we dig in to appreciate our clients' business to deliver tailored solutions. It is not always easy to do, but this is where the strength and value of the XBAND Extended Ecosystem is derived. We do not have to do it all today, but we are accountable for delivering the outcome.

TAG Cyber: I understand your team has also developed a security product that you offer to enterprise teams. Tell me about it.

XBAND: We are very fortunate at XBAND to have a team that is grounded and consistently innovating, working with the channel and our partners on client centric outcomes. I have supported thousands of CXOs to appreciate the consistent time and lack thereof that one can invest within an industry of over 3,000 technology providers.

What XBAND has enabled is a streamlined personified security stack based on the end user role. We have brought together many blue-chip, best-of-breed, and emerging technologies to help make the evaluation, contracting, implementation, and ongoing management easier for our clients, giving them back time to deliver value to their business.

We are able to perform as little or as much as our clients may require, from a fully managed outsourced security solution, to being a trusted technology provider with ongoing management responsibilities. Our security stack ranges from the business user, professional, executive, and advanced user. We have also architected vertical specific solutions for the healthcare and financial industries and remote call center agents as examples. XBAND's goal is to give back time to our clients while streamlining the process and empowering a competitive market position while delivering tangible financial and operational benefits.

AN INTERVIEW WITH WITH RICHARD MAGNAN, GENERAL COUNSEL AND CHIEF INFORMATION SECURITY OFFICER, RISING TIDE

CAN LAWYERS WHO DON'T UNDERSTAND TECH BE EFFECTIVE CYBER SECURITY STEWARDS?

If anyone is in a position to comment on problems in the relationship between in-house lawyers and their IT colleagues, it should be Richard Magnan. He has functioned in both roles. In fact, right now he is the general counsel and chief information security officer of Rising Tide, a company based in Schaffhausen, Switzerland, that runs two charitable foundations. After earning a bachelor's degree from the University of New Hampshire in mathematics and computer science, he joined the U.S. Air Force and worked as an applications programmer. The Air Force sent him to grad school for a master's in computer systems, and while there he developed an interest in software patents. Recognizing the value of having someone steeped in both disciplines, the Air Force sent him to Georgetown University Law Center. He wasn't sure which field he would pursue when he finished. He's spent much of his time since then living in Europe and alternating between the two—until at Rising Tide he found himself doing both. From that perch he's devoted considerable thought to the differences between the fields, why they often fail to mesh, and what can be done to fix that.

TAG Cyber: You speak English, some German, and a little French; mathematics and technology; and law. That's a lot of languages.

MAGNAN: Computer science and math have their own language, and law has its own. And the educational process is somewhat similar. It involves becoming comfortable with the terminology and the analytical process. Where they differ is that in mathematics, a problem usually has one right answer. In law it's almost the reverse. Sometimes there's no right answer. Sometimes there are multiple right answers. And one of the biggest transitions for me from math to law was in doing legal research, knowing when to stop looking for the exact answer by realizing that I wasn't going to find it.

TAG Cyber: You have expressed concern about lawyers who advise companies on cyber security. What concerns you?

MAGNAN: It's the ability to determine whether an IT solution that has been implemented, for example, to comply with the EU's General Data Protection Regulation (GDPR) is configured and used in a way that meets legal requirements. If you're looking at internal handling of personal data, and you're checking it against the GDPR, there are access controls, limitations on use, and record keeping requirements. There's a lot of software out there that claims to do that. And the IT department will be happy to help you get it. But then, after you get it, the legal department has to check how it's configured and used to ensure that it meets the legal requirements. And that's not something the IT department can do—at least not

by themselves. You need somebody who can look at the way IT implemented it, and how the business uses it, and compare that with the legal requirements. And this is where it seems that the legal community is not meeting the needs of the IT department or the business.

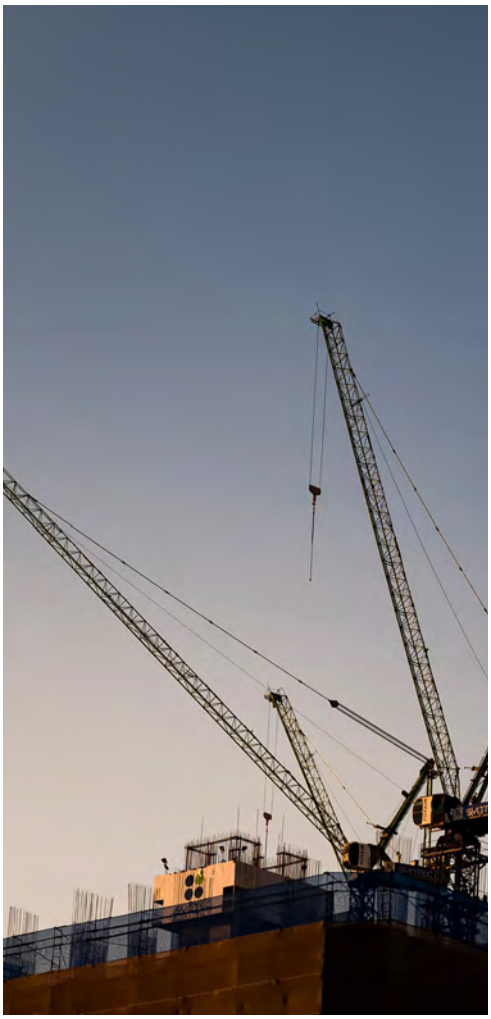
TAG Cyber: To be clear, is your concern about both cyber security lawyers and also those who advise companies about privacy?

MAGNAN: Yes. To me it's the same issue. I use the GDPR as an example because that's what I call internal controls or compliance implementation. That's different from the requirements for protecting the data against external intrusions. You don't have a single set of legal standards for both types of cyber security. Many statutes require "reasonable" or "adequate" security, but that's not enough specificity for IT to implement. So you have to look to case law, whether that's court cases or administrative agencies, like the Federal Trade Commission, or the SEC sanctioning companies for not meeting the standards. And in those cases you can see what the FTC says is the reasonable standard of care, either for administrative procedures or the major breach cases in the United States. The court proceedings are open and you can see the facts alleged in the complaint and the standard of care that allegedly wasn't met. This is a lawyer's expertise, this is their business. They routinely do this in other areas. Now you do the same thing in cyber security: You look at what the case law tells us, even if it hasn't gone to trial and the complaint is all you have. But it's better than nothing. You identify what the standard of care should be. And then you use that to work with your IT department to look at the risks with respect to your data—both the internal use of the data and the external risk of its being stolen by an intruder. And this is the essence of why legal and technology have to work together. It's to find the right combination of expenditures to meet the risk of data intrusion or data misuse.

Lawyers need to be able to ask at least a certain level of technical questions to be sure that the computer programs accurately implement the law.

TAG Cyber: Well, clearly the chief information security officer and the general counsel, or the general counsel's delegated lawyers, need to work together. If they are communicating regularly, why isn't that the solution to the problem?

MAGNAN: They're communicating, but they're communicating without the proper level of understanding. And that's primarily in the technology area. I'll give you an example. I teach data privacy, cyber security, and cyber law at two universities here in Switzerland. One of them is for experienced lawyers in a joint LLM-MBA program and another is a master's degree program for new lawyers. And in a class of about 15 students, primarily lawyers, maybe two or three will understand the technology. And I'm not expecting to make them programmers. But I am trying to teach them how data is stored and how it flows inside of a computer, because one way to look at data



privacy or data protection is that it's data management. It's knowing what data you have, what its value is, where it's stored, and how it's used. And then how it's finally purged so that it's not kept beyond its retention date. And so I try to teach just a little bit of computer architecture so that they can at least ask the right questions when they're working with the IT department. Lawyers need to be able to ask at least a certain level of technical questions to be sure that the computer programs accurately implement the law. And this is where I'm finding that the lawyers aren't able to do that. I've been doing this for about six years now, and it's surprising because for the most part these students are very intelligent and they can use any device you put in front of them with no trouble. But using a computer and understanding how it works, or at least how data flows, I've learned is considerably different.

TAG Cyber: What is the solution? Should there be some kind of license requirement or certification requirement before a lawyer is qualified to be a cyber security and privacy specialist?

MAGNAN: I'm not a fan of over-regulation, but there is an analogy with the U.S. Patent and Trademark Office. If you want to practice as a patent attorney in front of the USPTO, you have to pass a special exam. Maybe we need something like that to help us in this area. Right now the cyber security situation is bad and getting worse. We need to get the combination of legal and technical people into the companies to assess the risks, build up appropriate defenses, and protect the data both from internal and external threats. I'm confident we'll overcome this as the technology improves, as the education of the users improves, and as legal and IT work together to identify the risks and implement appropriate safeguards. But we're in a crisis that is becoming a catastrophe.

TAG Cyber: What is the danger to the company of ignoring the problem you've identified?

MAGNAN: It's financial risk for the business. If you need a certain type of protection, such as encryption, but you're buying something else, then the money on something else might help marginally, but it's not addressing your biggest risk. I previously ran the antipiracy/anticounterfeiting organization for an encryption systems company, and I actively pursued pirates and brought civil and criminal litigation against them. And then I spoke to the ones that we caught. And they said, "We're just looking for money. And we'll take the easiest path in. We're not computer scientists or engineers. It's trial and error. We just keep poking and prodding to see how we can get in." And so if we've got robust security in one area, but we've left the door open in the other area, they're going to find it. We need a systemwide view. And I think our cyber security technical people realize that, but the lawyers are focused on internal compliance, such as GDPR, and say, "OK, we've taken care of GDPR." But what about the defense against intruders? To me those are two separate

sets of technical solutions, and two separate sets of legal standards of care. And if you don't understand that, you're fixing one and leaving the other one open.

TAG Cyber: Europeans have had stricter rules on privacy than the United States for quite some time. Have you found that attitudes there about cyber security differ from those that we have here in the United States as well?

MAGNAN: Yes. This is a general reflection, but from talking to the law firms that I work with here, that's exactly the situation. The Europeans are more concerned about protecting their personal data than the U.S. And I don't mean that negatively towards the U.S. One of the differences—and this is taught in the European law schools—is the U.S. constitutional right to freedom of speech and the freedom to use information publicly in social media. That difference exists. But then the opposite difference appears to exist in cyber security. The U.S. corporations seem to be more concerned about cyber security, and more willing to bring in lawyers, computer scientists, and cyber security experts to prevent a breach than what we're seeing here in Europe. My European lawyer colleagues are saying that the amount of requests they're getting from businesses for cyber security support is much less than they would expect, certainly less than I would expect. And the question is why. The answer seems to be that European companies are more willing to accept a data breach and perhaps a fine for data loss as the cost of doing business. Whereas in the U.S., given the many types of lawsuits that can arise from a data breach, the cost is much higher to the companies there.

TAG Cyber: Any final words of advice you have to offer the legal communities in the U.S. or Europe?

MAGNAN: For both legal and technical communities, I have a concern about cyber security. Where's the deterrence? As I mentioned, I created a corporate antipiracy team focused on internet crimes. And when I talked to the pirates, they said the path of least resistance is what they're looking for. And one aspect of resistance is whether they would be sued. We saw a substantial decline in breaches and piracy after a few years of prosecuting them, because there was deterrence. And we were successfully suing the highest level criminals—the importers of the illegal systems, the manufacturers of the illegal systems. This was not prosecuting cases against the end users of the illegal systems. The question today is: How do we prosecute the ultimate criminals? We need enforcement. It's tough. It takes time. And we need international cooperation. But it can succeed. We've got to deter people who are making a lot of money in relative immunity today from practicing their illegal profession.

ANALYST REPORTS

TAG CYBER

Data Sharding for Back-End Cloud Security

Data sharding for back-end cloud security addresses the threat of compromised insiders with privileged access. The method disaggregates, separates, and obfuscates data so that insiders within cloud service infrastructure cannot make sense of stored assets.

Prepared by
Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
eamoroso@tag-cyber.com

Version 1.0
April 27, 2020

Introduction

The challenge of protecting enterprise assets in public cloud infrastructure has emerged as one of the top concerns for the modern Chief Information Security Officer (CISO). This contrasts with earlier debates about whether to allow for such external hosting of internal resources. Those discussions have completed – and almost uniform agreement now exists that cloud infrastructure will be used for at least some applications, often in hybrid mode.

The cloud security challenge is typically represented as follows: An employee needs access to an enterprise resource hosted on a public cloud. Since the cloud is Internet accessible, the access path from the employee is publicly visible to attackers. End-to-end controls such as cloud access security brokers (CASB), multi-factor authenticated login, and microsegmented workload architectures are thus placed in-line to reduce cloud access risk.

The primary threat being addressed with this approach involves non-authorized individuals somehow gaining access to the cloud-hosted resource. This might involve use of credential theft, identity spoofing, or some other malicious means to trick the cloud host into believing that the request is valid. It's a tough risk to manage, because many attacks, such as credential theft, are performed outside the purview of the cloud.

In this report, we examine a related threat, but one that could be more serious, and that is almost certainly being paid less attention by enterprise cyber security practitioners. The risk involves *back-end access* to cloud-resident data by individuals, groups, and even automation without proper authorization or purpose. Many of the use-cases for back-end threats involve compromised administrators, but unintended or erroneous actions are also common.

Front-End Cloud Security Protection

As alluded to above, the most familiar security approach used to protect cloud infrastructure involves *front-end* protection, because it addresses the normal interface used by employees and other authorized individuals for access to cloud-hosted resources. The protections sit in the end-to-end access path to authenticate users, detect anomalies, generate telemetry, support mitigation, and provide a means for performing incident response and forensics.

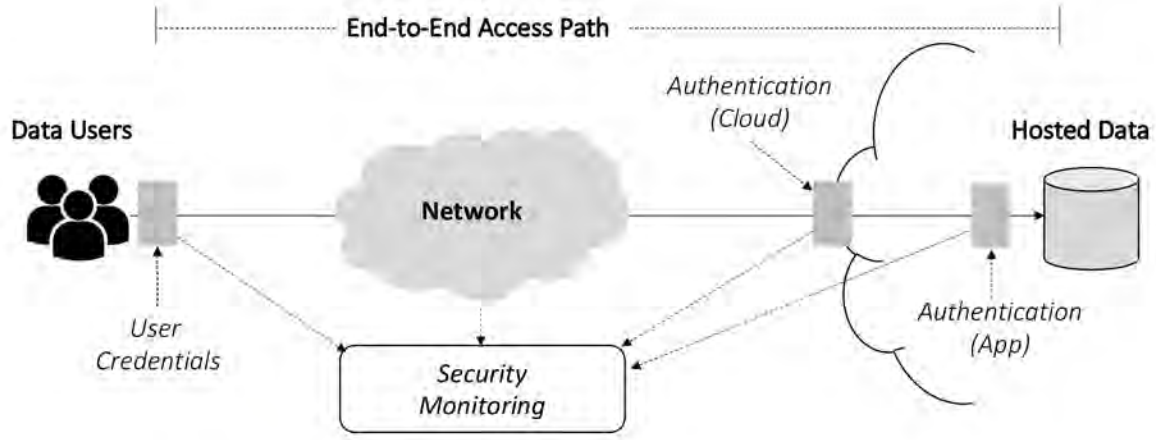


Figure 1. Front-End Security Protection for Cloud

It is worth mentioning that this front-end view also includes automated systems accessing cloud assets. Machine-to-machine transactions increasingly use cloud systems through an application programming interface (API). The security protections for APIs often include comparable controls for human users. These include gateways, authentication, and monitoring, and can be used for both IT and operational technology (OT) resources in cloud.

This view does, however, ignore a significant aspect of cyber risk that is arguably more intense in its consequence for cloud-hosted resources. This aspect involves the administration of cloud infrastructure, including the management of resources, assets, and data. The challenge of protecting administrative access can be described accurately as back-end protection, because it does not sit in-line with normal user or even machine-based access over an API.

Back-End Cloud Security Protection

The functions typically involved in back-end access to cloud-hosted resources include the day-to-day tasks that are necessary to ensure proper hosting and a good user experience. This can include performance tunings, patch management, software updates, new feature introduction, and so on. These tasks generally require the highest level of privilege (e.g., Unix root) so the side-effects of an administrator becoming disgruntled or just making an error can be significant.

The types of security controls that are common to reduce risk in back-end cloud infrastructure settings often parallel the ones used to protect front-end access, but that are simply re-positioned for administrative access. This includes authentication, privilege management, and activity monitoring. These are excellent controls to detect improper access to administrative accounts, but they are weak controls to deal with a compromised or hacked administrator.

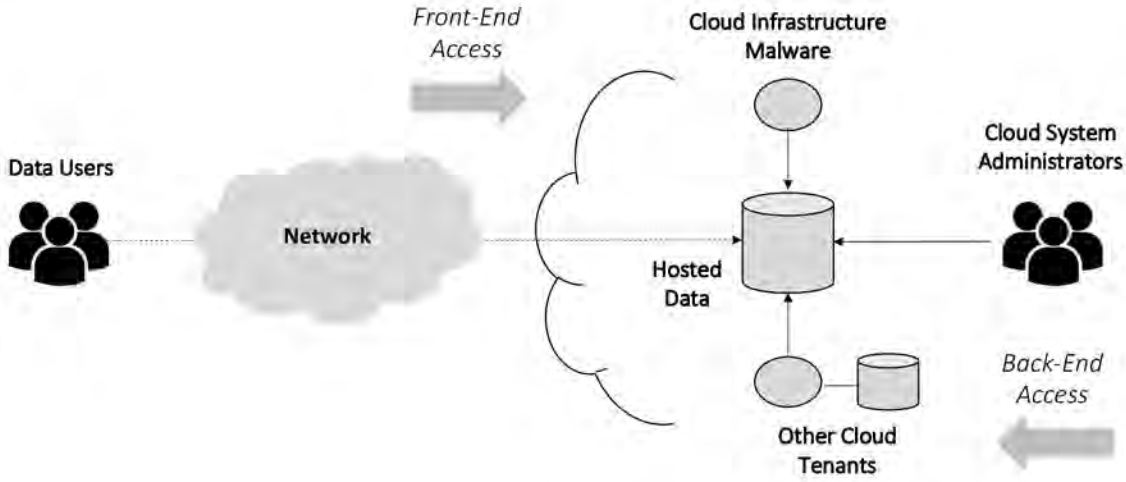


Figure 2. Back-End Security Threats for Cloud

To address the problem of rogue, disgruntled, or compromised cloud administrators, several options emerge. One involves strict contract management with public cloud services, with clearly defined penalties if evidence of insider attacks emerges. Another control involves the use of logs to uncover evidence of insider threats. Both of these approaches, however, might be covered up or suppressed by a competent malicious insider with high privilege.

The more common problem, however, involves non-malicious staff erroneously accessing, handling, or using cloud-resident resources. Errors during normal administration, maintenance update, patching, rehosting, and other tasks can easily result in a serious data compromise. The security controls to address such risk must be designed to deal with these common, but inadvertent problems.

What is needed, however, is a stricter control, one that cannot be subverted by a rogue or sloppy insider. This is where the emerging protection technique known as *data sharding* (or just sharding) has become increasingly important. The algorithms associated with sharding are relatively mature, but only recently have they been applied to modern protection of cloud-hosted resources.

Data Sharding to Reduce Back-End Cloud Risk

The general method of data sharding can be easily described schematically in terms of three algorithmic components: First, sharding involves disaggregating a given file or other asset into a set of smaller pieces. Second, the method involves separating these assets in manner that makes it difficult for any single hosting source to put the pieces together. Finally, the method involves obfuscating the disaggregated, separated asset pieces.

This three-step process offers an excellent means for securely storing sensitive data into the cloud. Furthermore, it supports the hosting of such data across disparate multi-cloud environments, thus dramatically reducing any back-end data access risk from unauthorized or unintended cloud actions. Tools are required obviously to retrieve and re-assemble the stored data for use by authorized individuals or data owners.

This last point is important to emphasize: Data sharding is not designed for storage in a passive manner, but rather for active hosting with query, access, and normal usage by users through cloud interfaces and processes through APIs. The algorithms must be designed with a retrieval capability that can combine and aggregate the data that has gone through the data sharding process.

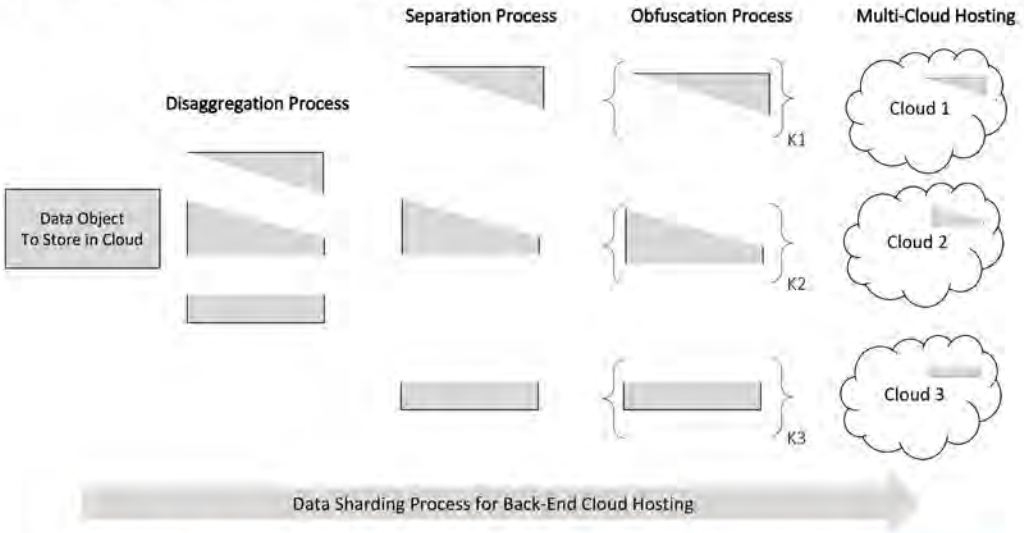


Figure 3. General Schematic Description of Data Sharding

The cyber security advantages of data sharding in the context of back-end cloud access include the following:

- *Supports Multi-Cloud Security* – When data is sharded across multiple target hosting locations, a powerful level of multi-cloud security can be achieved. This is helpful in many compliance settings, especially where the insider threat for externally hosted data is viewed as particularly intense. One might imagine financial services companies finding multi-cloud security controls important.

- *Complements Encryption* – Encryption of data before hosting into cloud is a common application-level control for hosted resources. This method is compatible with data sharding and can be used to provide layered security. The obfuscation involved in sharding can be over-laid onto any existing encryption without causing any functional issues.

- *Consistent with Multi-Person Controls* – The use of multi-person controls could be used for back-end access for hosted data sharding. That is, if administrators needed access to sharded data, then this could be accomplished through the design and development of tools that would aggregate and re-assemble the multi-cloud hosted data, but that could easily be only allowed with multiple administrators.

The motivation behind data sharding to reduce back-end cloud access threat is that hosted data is only useful if it can be retrieved and interpreted. If individual shards are neither complete nor meaningful when stored, then the threat is reduced. An additional consideration is that some vendors offer granular algorithms to manage the size and scope of the sharding – including, for example, micro-sharding options. Buyers should review options with their selected vendor.

Enterprise Recommendations

Any enterprise security team with responsibility to reduce risk in cloud-hosted infrastructure would be wise to begin examining commercial solutions in this emerging area. The TAG Cyber team provides regular guidance on excellent options for data sharding vendors, but since this is a new area, vendor mixes change frequently. Some of the commercial data sharding solutions examined for this work include the following:

Altibase (provides sharding for client and server-side database operations), *MongoDB* (includes sharding in its database solutions), and *ShardSecure* (start-up that provides a general data sharding solution for multi-cloud).

About TAG Cyber

Founded in 2016 by Dr. Edward Amoroso, retired Chief Security Officer for AT&T, Manhattan-based *TAG Cyber* democratizes cyber security industry research and advisory through high-quality reports, guidance, and information accessible to a wide expert audience. TAG Cyber helps close the communications gap between enterprise practitioners and security vendors. TAG Cyber also offers consultation and research subscriptions for enterprise practitioners.

TAG CYBER

Evolution of the Zero Trust Model for Cyber Security

Prepared by
Dr. Edward G. Amoroso
CEO, TAG Cyber and Research Professor, NYU
eamoroso@tag-cyber.com

Thirty years ago, a researcher wrote a small piece of software that saved his company from a cyber attack by a college student. The software examined inbound TCP packets for ACK=0, which denoted the start of a session. If a new session looked funny for any reason, then the packet was dropped. Weird source IP addresses or unauthorized destination services were typical justifications for disallowing inbound packets. The code was well-written and it worked.

The code author was named Bill Cheswick and the company saved was Bell Laboratories. The college student was Bob Morris Jr. and his attack was the Internet Worm of 1988. (In an ironic twist, Bob Morris Jr. had a famous father of the same name who'd helped invent Unix at Bell Laboratories). And as for the small piece of software written by Bill Cheswick – well, it was arguably the first working enterprise firewall. (And no, the company did not patent the idea.)

Other organizations not running an early firewall were infected with the Morris worm because they assumed a so-called *full trust* model between entities on the internet. Remember that when the internet was invented, the presumption was that this new forum was to be used solely for trusted communication and sharing. Basic cooperative norms existed across the early internet, and were respected by individuals, groups, companies, and other entities.

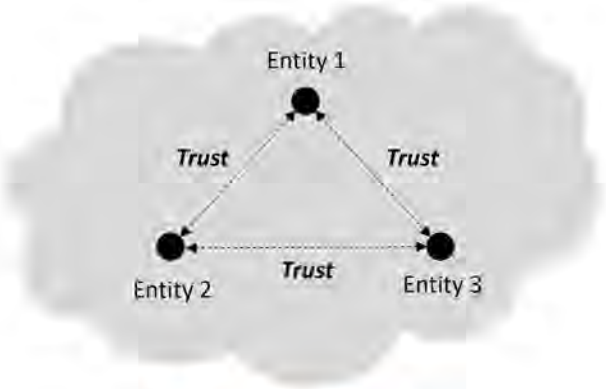


Figure 1. Full Trust Model

But by the mid-1980's, it was apparent that the optional norms and procedural controls on the internet – usually to be followed voluntarily by network operators and systems administrators – were insufficient to secure the growing number of critical functions being hosted on this new global infrastructure. Individual and group hacking soon emerged as a serious menace – and the Morris worm exemplified the cascading power of well-defined attacks.

Such security issues ushered in an era of *perimeter networking*. That is, soon every organization in the world created a firewall-based bunker, which provided a *partial trust* model between entities inside and outside an enterprise. Thus, if an entity was located inside the firewall, then it could trust any other entities within the perimeter – users, desktops, servers, printers, applications, and so on. If an entity was outside, however, then it was not to be trusted.

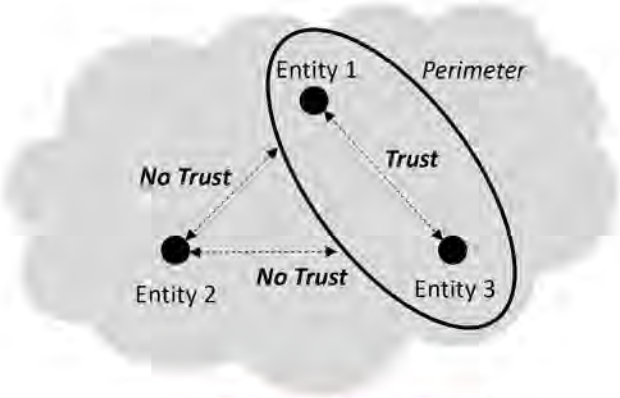


Figure 2. Partial Trust Model

This partial trust model has driven enterprise security for three decades. It's severe drawbacks, however, soon became evident. First, an entity could be inside the firewall, but also be malware-laden or disgruntled. Second, if an entity wanted to connect to the world, then the perimeter needed to allow email, remote access, and web – all open doors for hacking. And third, any mobile-connected device could wirelessly bypass any enterprise firewall.

To address these weaknesses, enterprise security teams completely redesigned the original perimeter concept, opting for a new model that combines the great modern themes of today – namely: *cloud, mobility,* and *apps*. This new model is based on the idea of mobile devices accessing cloud-hosted apps without the need for a perimeter. The resulting device-to-cloud operation produced something now referred to as a *zero trust model*.

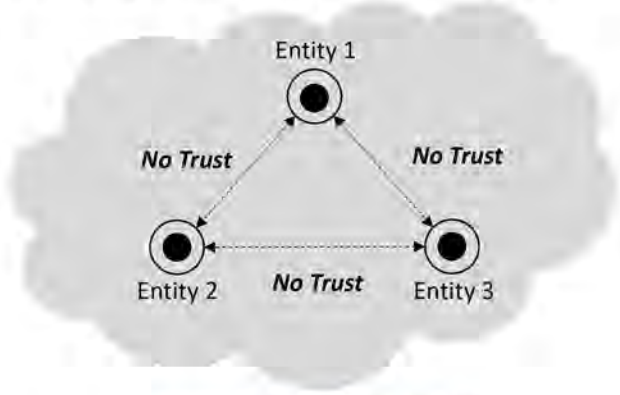


Figure 3. Zero Trust Model

To implement zero trust cyber security, represented by the little circles around each entity in figure 3, four components are required: *Devices, transport, cloud,* and *apps*. Let's examine the role of each in the context of a typical, modern enterprise deployment:

Devices. The security obligations for device stewards in a zero trust environment involve ensuring strong authentication to the device, protecting the mobile device operating system and application environment from malware, and establishing a secure launch point for connectivity to cloud-hosted apps.

Transport. The security obligations for transport infrastructure providers in a zero trust environment involve maintaining highly available communications, since device-to-cloud services are the new backbone for business and personal use, and supporting flexible means for protecting networks from attacks such as DDOS.

Cloud. The security obligations for cloud hosting providers[1] in a zero trust environment involve providing microsegmentation for workloads, as well as supporting security and regulatory compliance demands imposed on any external hosting of critical enterprise applications. The cloud must also support secure device connectivity and network access control.

Apps. The security obligations for applications in a zero trust model environment involve supporting highly secure code, integrating security connectors to provide telemetry to cloud-hosted tools such as SIEMs, supporting secure device connectivity, and implementing proper access management and data security for any stored sensitive information.

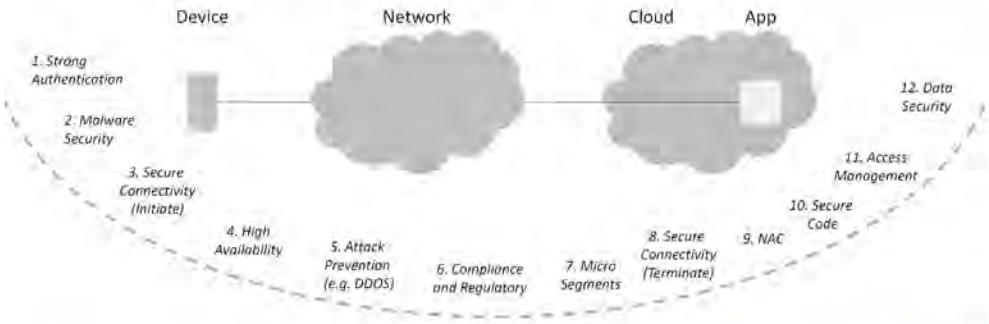


Figure 4. Security Controls for Device-to-Cloud in a Zero Trust Environment

An excellent example of a zero trust implementation is the Google BeyondCorp concept used for enterprise networking at the company[2]. The goal in Google's secure enterprise design is to remove dependency on its perimeter. Instead, a device-to-enterprise scheme uses company-provisioned device access to Google network infrastructure for secure access to required business apps. Below are the salient aspects of this design:

Access Based on Credentials. In BeyondCorp, direct access is only permitted for devices that are procured and managed by Google. Device inventory is tracked, and configuration changes to devices are maintained in a meta-inventory. Certificates are issued and stored in trusted platform module (TPM) hardware on devices, and are referenced in an inventory database. A qualification process determines if an endpoint device is secure enough for access.

Access and Encryption. Access management is the central function for the BeyondCorp design, and is implemented based on the attributes of the requesting user, any relevant group memberships, and applicable HR-related job functions. Single sign-on (SSO) is supported using short-lived tokens generated for use during sessions. All sessions originated at a provisioned device are also encrypted.

Untrusted Network. Google runs an unprivileged network for device access that is essentially public but that is located in private Google address space. Only minimal external connectivity is included on this

[1] Zero trust connectivity to a corporate enterprise results in the traditional "enterprise LAN" being viewed as a remotely accessible cloud. In this way, device-to-cloud access for a corporate app is no different conceptually than device-to-cloud access to Facebook. The difference is the access management at the cloud or app destination.

[2] See "BeyondCorp: A New Approach to Enterprise Security," by Rory Ward, and Betsy Byer. Presented in ;login, December 2014. https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf

network to DNS, NTP, DHCP, and Puppet. RADIUS used to provide network access control (NAC) coordination to the desired VLAN for access to the Google application being requested.

Identical Local and Remote User Experience. The operational result of BeyondCorp is that the session experience for users accessing Google apps locally is essentially the same as for users accessing the same apps remotely. In this way, BeyondCorp elegantly removes the need for an enterprise perimeter, which implies all the security and operational benefits of a zero trust computing environment.

TAG CYBER

A Process to Implement Zero Trust Access

A simple iterative process is introduced to help guide IT, network, and cyber security teams in the introduction of zero trust access to their enterprise. The process starts with quick win selection of systems, applications, or workloads, followed by a stepwise implementation toward the target goal.

Prepared by

Katherine Teitler
Senior Analyst, TAG Cyber
kteitler@tag-cyber.com

Edward Amoroso
Lead Analyst, TAG Cyber
eamoroso@tag-cyber.com

Introduction

Zero trust access involves protecting enterprise resources without reliance upon any firewall-based perimeter, although firewalls can still be helpful as part of your overall security strategy. With zero trust access, no user or entity is trusted by default to access enterprise resources based solely on their internal network positioning. Instead, access to enterprise applications, systems, and services requires explicit identification and authentication, even if such access is made laterally across an enterprise local area network (LAN). This approach greatly reduces enterprise security risk.

Because common IT and security initiatives such as cloud workload deployment and remote work-from-home support serve as building blocks, it turns out that implementation of zero trust access is often much easier than expected. This report provides a simple plan that can help develop an implementation framework to achieve zero trust. The plan includes four steps that iterate from a baseline architecture to one more consistent with improved security.

Plan to Implement Zero Trust Access

The process to implement zero trust access involves four simple, iterative steps that can be used as the basis for a local plan. The presumption is that the iterations would proceed from a series of initial quick win deployments in which select enterprise workloads, systems, or applications are transitioned from their legacy implementation to one supporting zero trust. The quick win approach is particularly well-suited here because it allows teams to build an experience based on simpler initial transition cases.

The four steps are designed specifically to avoid disruption throughout the zero trust transition, while also ensuring that positive changes are not offset by negative process issues which could have been avoided. These steps involve creating an inventory of assets involved in a given transition, identifying the applicable stakeholders, driving the transition based on an explicit plan, and then adjusting any applicable business processes (see Figure 1).

Figure 1. Iterative Steps for Managers Implementing Zero Trust Access

Each of these steps in the proposed iterative process toward zero trust are explained and illustrated in the sections below.

Step 1: Create an Inventory of Assets

Upon each iteration of the simple process for implementing zero trust access, it is necessary for IT and security teams to take a targeted inventory of applicable assets involved in the transition. The complexity of this inventory task will track directly with the scale, scope, reach, and features of the workload selected for transition to zero trust. By focusing the initial work on quick win projects with relatively simple functionality, this inventory step will likely be quite straightforward.

Typical assets to be identified in the inventory step include (1) the application, system, or workload selected for the transition step, (2) a list of applicable end users, (3) a list of all back-end system dependencies such as directories or databases, (4) a list of applicable existing security controls, and (5) identification of all policies in place for access to the target. Such inventory will help the IT and security teams ensure that the zero trust transition covers all relevant use cases for the targeted asset.

Step 2: Identify Key Stakeholders

While the IT and security teams tasked with managing to zero trust will always be key stakeholders in the process, each iteration will also require support from various other individuals and teams in the organization. The most common stakeholders include the owners of the application, system, or workload targeted for transition. They are necessary to provide the detailed context and support required to ensure a smooth shift from legacy to zero trust access.

Having disparate and unwieldy policies for each network segment can make managing the network complex and overwhelming.

While it might not be necessary to create formal advisory or governance groups to oversee the zero trust access transition process, teams should consider including some organizational structure during each iteration. IT and security management would be wise to focus on keeping stakeholders directly involved and informed during the transition step. This should be done consistent with the local norms for such cooperation, including use of any tools for information sharing.

In addition to key stakeholders, organizations should also seek vendor partners with the desired types of zero trust access functional support. It is important to note that new technologies may have stronger security capabilities that should be evaluated for inclusion in the new zero trust access solution. For example, teams might require more refined access control policies in the platforms they select. In many cases, having disparate and unwieldy policies for each network segment can make managing the network complex and overwhelming, whether on-premises or in a cloud, hybrid cloud, or multi-cloud setting, so selecting a vendor partner who can help simplify and consolidate your access security can be a significant advantage.

In addition, vendor solutions might be selected that unify access control using single sign-on, with consistent enforcement policies across networks and support for administrators to audit policies from a central console. Zero trust access controls that continuously assess the validity requests based on multiple attributes such as IP address, device type, and OS will help remove the need for humans to approve or deny each request manually.

Step 3: Create a Zero Trust Architecture Plan

An important consideration in the process toward implementation of zero trust is that the target architecture will be achieved in an iterative, stepwise manner. This implies that the existing perimeter-based legacy (perhaps already in a hybrid cloud mode) will follow a series of transitions for select applications, systems, and workloads – eventually arriving at the desired state. This is helpful, because it supports early quick wins and allows for experience-based adjustment to the process.

The most important property to be maintained through transition to zero trust access involves dissolution of any default authorizations based on local positioning on the enterprise network.

While each step will require a plan that takes into account the specific functionality, user base, functional controls, and mission purpose of the selected application, system, or workload, some generic guidelines can be identified to assist IT and security engineers during the transition. Such generic assistance usually involves clear description of the existing precondition state along with guidance on the target state with zero trust access. This is especially important because zero trust access can have more comprehensive security policies that will better protect your resources.

Regardless of the specific plans created for each successive step, the most important property to be maintained through transition to zero trust access involves dissolution of any default authorizations based on local positioning on the enterprise network. That is, every step in the proposed process to zero trust will begin with a perimeter-based access architecture and will result in a zero trust arrangement devoid of reliance on a perimeter. The diagram in Figure 2 shows a typical generic transition.

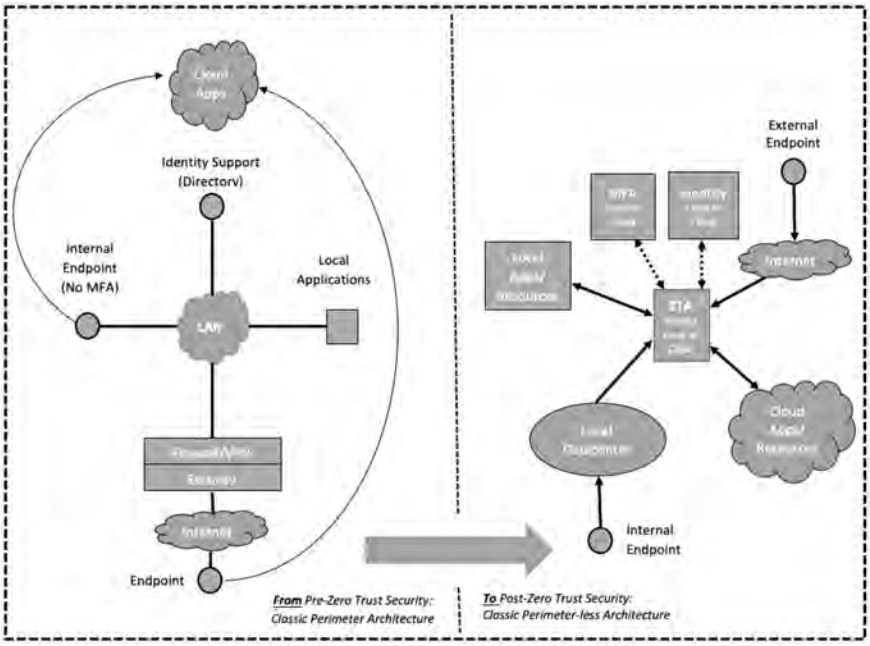


Figure 2: Typical Zero Trust Access Architecture Plan Transition for an Application

Step 4: Adjust Business Processes for Zero Trust

While it might be tempting to consider the zero trust transition complete once the new functionality has been achieved, IT and security teams have the obligation to ensure that any changes do not require adjustments to applicable business processes. Training and user support teams, for example, must be made aware of any new zero trust set-ups, and this could require that they amend or adjust applicable processes that support the user base.

Teams should expect, as the early quick wins are completed during the stepwise implementation of zero trust, that this business process adjustment step will gradually become a lesser concern. That is, once support teams such as help desks and IT administration groups are made aware of the ongoing transition, it will become easier to provide information on successive applications, systems, and workloads undergoing a shift to zero trust.

The Bottom Line: Simplify, Consolidate, Strengthen

As resources are moved to a zero trust access architecture, teams will be able to greatly reduce the complexity of their infrastructure and close more ports to the outside world, strengthening security across the enterprise. Stronger controls created by zero trust access will provide targeted and secure microsegmentation of resources that make the lives of both end users and admins alike easier. Finally, for the first time, teams will be able to provide centralized reporting and auditing of all access to local and cloud resources and applications.

TAG CYBER

Understanding API Security

An introduction to API security threats, challenges, and solutions is provided for participants in software development, operations, and protection. The Cequence platform demonstrates the API security concepts for live enterprise deployments.

Prepared by
Dr. Edward G. Amoroso
CEO, TAG Cyber and Research Professor, NYU
eamoroso@tag-cyber.com

COMMISIONED BY
CEQUENCE SECURITY

Version 6.0
April 20, 2020

Purpose of this eBook

Researching the wide range of application programming interface (API) security alternatives can be confusing – even to seasoned experts. This eBook is written with the goal of helping all types of readers better understand the pros and cons of the various modern approaches to protecting APIs from cyber security risks. The material is intended to help enterprise security and software development teams develop and maintain a consistent protection philosophy.

The target reader includes software developers who depend on and use APIs every day, as well as technical managers who might have responsibility for API security in their organization. The target reader also includes, however, technical-minded individuals possessing little experience with APIs, but who are nevertheless interested in the security aspects of this important issue. We try to describe the API security concepts in a manner accessible to each type of reader.

Introduction to APIs

The typical user of network and Internet services tends to think of *computer interfaces* in terms of screens, keyboards, monitors, and the like. These interfaces are the visible means by which systems exchange information with human users,and they have advanced rapidly in recent years. The touch screen from Apple, for example, emerged only a decade ago, and a generation of youngsters barely remembers what the world was like before such useful capability existed.

But there is another type of interface that exists in computing, perhaps more hidden to the everyday user. This other type of interface is how software programs communicate with one another. For many years, this process was poorly specified, with programmers inventing protocols for something called inter-process communication (IPC). An early operating system from Bell Laboratories called Unix, which now serves as the base of both Apple iOS and Android, made IPC designs easier, but they were non-standard.

By 2000, the industry decided that these software-to-software interfaces needed to become more open and standard. Such technical decision became the genesis of what we now refer to as an *application programming interface* or more commonly – API. Recognize that an API provides a standard interface through which two software programs, also referred to commonly as processes, can communicate, share messages, or managed shared memory.

More specifically, an API is an interface which makes software services available to workloads or applications for bidirectional communication and message sharing. APIs are also commonly used to share memory between different processes. An API is stateless in nature, and will commonly include all the information needed to complete a transaction, unlike a web form that may require multiple transactions for processes like user registration.

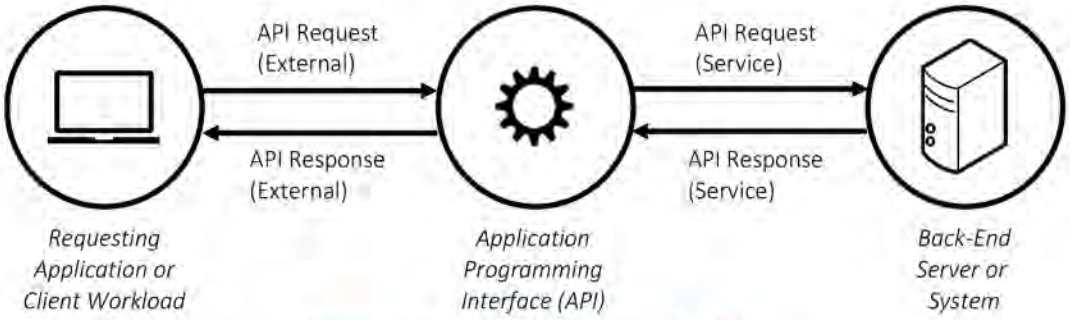


Figure 1: General API Model

Unix Operating System IPC

Roughly half a century ago, researchers Ken Thomson and Dennis Ritchie of Bell Laboratories initiated a project to build a multitasking operating system for use inside AT&T. Despite such relatively modest original goals, the so-named Unix software and associated design philosophy that they produced have served as the technical base for virtually every successful commercial operating system since. Linux and Android are direct derivatives, whereas iOS and Windows are massively influenced by Unix.

An important design consideration for the Unix operating system involved the need to create an inter-process communication (IPC) mechanism that would allow for data sharing and message passing between computer programs. Thompson and Ritchie were influenced by many rapidly evolving technical concepts being designed at the time in the computer science community. This included the emergence of producer-consumer models, as well as new methods for distributed computing.

The Unix IPC approach can be viewed as an early attempt to address many of the issues now covered by application programming interfaces (APIs). Both are concerned with the need to modularize, standardize, and simplify the manner in which data or messages are shared between cooperating processes. The big difference, obviously, is that modern APIs benefit from the massive scale that comes with the Internet. Original Unix efforts were local and operating system-specific.

Anyone interested in understanding better the origins of distributed inter-process communication would be advised to read some of the original materials from the Unix designers. Dennis Ritchie reflects on the local environment that served to help prompt the Unix design in this paper. Additionally, Ken Thomson displays the elegance and fun associated with the Unix philosophy of programming in his wonderful Turing lecture address.

Growth of APIs

When Salesforce and eBay became the first major Internet players to focus on making their systems available to external programs via an API (versus traditional means such as command line interface (CLI)), they ushered in a new era of so-called *open computing*. What this meant was that rather than close off their software to the external world, as was the general practice before 2000, open computing encouraged systems to allow for others to have their software connect directly. As one might guess, the result was explosive growth on the Internet.

Imagine, for example, how difficult it might have been for Amazon (which published their first API just after Salesforce and eBay), to have grown so quickly if they had walled off their applications from other systems on the Internet. Without open computing, they would have had trouble integrating security protections, purchasing partners, supply chain management, authentication services, and on and on. All the things we have come to expect from a modern Internet service now depend on open computing and APIs.

Invention of the REST API

In 2000, Roy Fielding completed his PhD at the University of California at Irvine. His PhD thesis, unlike most such works, includes arguably the first meaningful description of what we would now refer to as an application programming interface (API). Specifically, "Architectural Styles and the Design of Network-Based Software Architectures" ushered in a new era of programming style for the web, using a technique referred to as Representational State Transfer or REST.

The specific details of REST APIs are beyond the scope of this short summary, but we can outline some of the more salient constraints that help define this uniform set of software connector interfaces. The first design constraint in the REST style of programming involves stateless processing for all client-server interactions. By reducing API requests to a single transaction (versus including history), it become much easier to create proper "visibility, reliability, and scalability," as Fielding explains in his thesis.

Additionally, cache constraints are added to the REST API model to reduce the latency of interactions. The most central design constraint of REST APIs, however, is the uniformity of the interfaces that is inherent in the overall design. This is complemented by design layering, which reduces the complexity at a given layer (via abstraction of lower layers) and code-on-demand, which "allows client functionality to be extended by downloading and executing code in the form of applets or scripts," again, as Fielding describes in his work.

The implications of REST API design from Fielding's PhD proposal were immediately felt across the entire web community. Soon after publication of the thesis, companies like Salesforce and eBay began to demonstrate how the programming style as associated uniform connector model could substantially increase their reach to the web. They quickly saw that APIs not only made their interfaces more standard, but made the services they provided to the external community much more accessible and more popular.

More recently, API usage has seen even greater exponential growth driven by several factors – the first of which is the ubiquitous *mobile device*. By making the Internet accessible anywhere, anytime, and to everyone – mobility increased the demand for more connected and integrated services. It's hard to imagine API-heavy services such as Salesforce, eBay, and Amazon experiencing such great success without the explosion of mobile device usage.

Additional factors driving API usage might be less familiar to normal users. Software designers have moved, for example, to modular applications, which makes it easier for them to add features more quickly and to iterate more rapidly during software development to create standard interfaces. Network architects have also begun to adopt an approach known as a *service mesh*, which depends on hyper-connectivity between software workloads. As one might expect, this connectivity is achieved through the use of APIs.

The API explosion is also driven by several business-oriented factors. First, enterprises are moving away from large monolithic applications that are updated annually at best. Instead, legacy and new applications are being broken into small, independently functional components, often rolled out as container-based microservices. The resulting application components and microservices work together to deliver the same functionality as the monolithic applications.

OWASP Top Ten Risks

The Open Web Application Security Project (OWASP) Foundation was created to improve the security of software through community-led software initiatives, local chapter work led by members, and many different conferences. Its most famous product is the so-called OWASP top ten risks, which are published to help software developers avoid the most common risks in the creation and use of web applications. A description of the top ten OWASP risks is listed below, and taken directly from the OWASP Website at https://owasp.org/www-project-top-ten/:

1. Injection. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

2. Broken Authentication. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

3. Sensitive Data Exposure. Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

4. XML External Entities (XXE). Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

5. Broken Access Control. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

6. Security Misconfiguration. Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

7. Cross-Site Scripting XSS. XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

8. Insecure Deserialization. Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

9. Using Components with Known Vulnerabilities. Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

10. Insufficient Logging & Monitoring. Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Holding all of this together, of course, are the APIs that allow for communication between processes, bi-directional sharing of data, and real-time provision of services. By serving as the bridge between applications, components, microservices, and other containerized workloads, APIs can be viewed as integrating large portions of the Internet, including eCommerce, supply chain processing, enterprise business interactions, and other components of the modern digital economy.

At a more technical level, the factors that have helped to make APIs so pervasive in the design and implementation of Internet services include the following:

- *Support for DevOPs* – Iterative development methodologies such as DevOps, DevSecOps, and Agile enable teams to push incremental changes directly to customers instead of using long development and assurance cycles.

Security in DevOps

The waterfall model of software development has become a victim of time. That is, the duration between when software requirements are defined and the time functional code is delivered has become too lengthy for most practical environments. In fact, by the time a waterfall project gets around to coding, the requirements have often changed so much as to render the activity irrelevant. Because requirements changes usually originate with end-users, the situation is unlikely to change.

To address this accelerated lifecycle, so-called DevOps processes have emerged in the software community. Designed to address the increasing pace of requirements change, DevOps involves rapidly-organized and quickly-executed tasks designed to produce and deploy new requirements quickly. Integration between coders (the Dev part) and production users (the Ops part) creates a never-ending spiral cycle of software development that is best performed with a maximum of automated support.

Introducing security into DevOps became an obvious concern once DevOps processes were applied to critical system development efforts. Experts saw this as an immediate challenge, because many security tasks have the inherent result of slowing down deployments due to a traditional reliance on change control processes. This produced an immediate collision between security and the obvious DevOps objective of moving as quickly as possible.

The solution to the DevOps security challenge is automation. Only through the introduction of automated controls for tasks such as security testing, code scanning, control monitoring, and activity logging – can the speed of DevOps be maintained, while also ensuring that vulnerabilities are not being introduced as a result of the process. Obviously, buggy code with exploitable breaches will continue to emerge from DevOps, but these should not be introduced as a result of the process.

One interesting and curious note worth mentioning is that the community has not agreed on a standard nomenclature for secure DevOps processes. One might find references to DevSecOps, SecDevOps, and DevOpsSec – and this author has no good advice for identifying the differences. Readers are advised to engage with the security team early in the application development process to foster a tight working relationship.

- *On-Demand Flexibility* – Modern application hosting requires the ability to scale services up or down, on-demand, and in a cost-effective and efficient manner, to handle changes in usage patterns, such as seasonally-based demand.

- *Development Frameworks* – Technology adoption trends such as increased use of cloud, containers and orchestration (such as Kubernetes), and management frameworks (such as Istio) make it easier to develop and deploy API-based microservices at scale.

- *Diverse Ecosystem* – Partner ecosystem expansion, enabled by API-based microservices enable aggregators, suppliers, and external developers use to grow their business without replicating functionality. These APIs are well-documented and publicly-available, as evidenced by the massive directory of more than 23,000 APIs that one can find on the Internet (see https://www.programmableweb.com/).

The increased adoption of APIs is thus great news for businesses, but introduces corresponding challenges for security professionals. Enterprise teams who might have been tasked previously, for example, with protecting a handful of applications, might now be suddenly responsible for protecting hundreds if not thousands of public-facing APIs with a range of cyber security risks. As a result, API security has become a top-of-mind issue for most CISOs.

Threats to APIs

The many benefits that APIs bring to the software and application development communities – namely, that they are well documented, publicly available, standard, ubiquitous, efficient, and easy to use – are now being leveraged by bad actors to execute high profile attacks against public-facing applications. For example, we know that developers can use APIs to connect resources like web registration forms to many different backend systems. The resultant flexibility for tasks like backend update also provide support for automated attacks.

The security conundrum for APIs is that whereas most practitioners would recommend design decisions that make resources more hidden and less available, successful deployment of APIs demands willingness to focus on making resources open and available. This helps explain the attention on this aspect of modern computing, and why it is so important for security teams to identify good risk mitigation strategies for API usage.

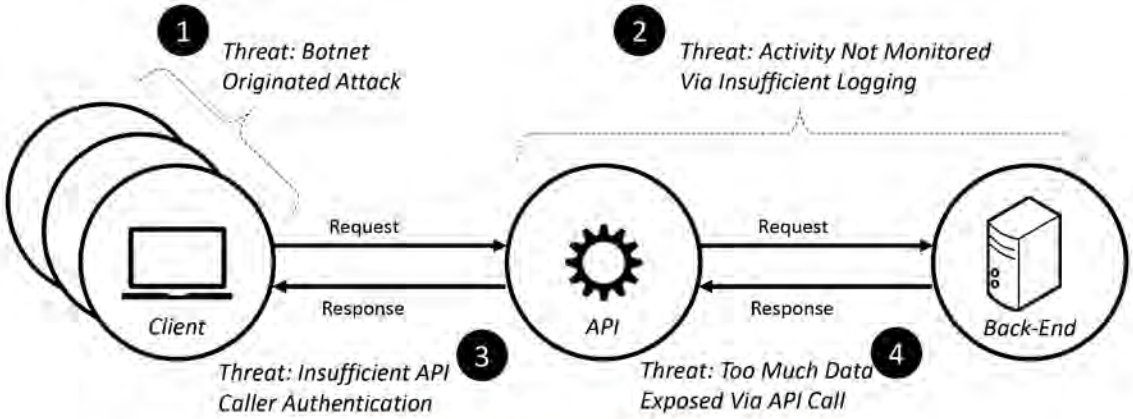


Figure 2: Security Threats to APIs

OWASP Risks to APIs

In addition to its focus on risks to general software applications, OWASP has also provided useful guidance for API developers to reduce security risk in their implementations. Given the prominence of the OWASP organization in the software community, it is worth reviewing the 2019 Top 10 API Security Risks (with wording taken from the OWASP website):

1. Broken Object Level Authorization. APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface level access control issue. Object level authorization checks should be considered in every function that accesses a data source using an input from the user.

2. Broken User Authentication. Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user compromises API security overall.

3. Excessive Data Exposure. Looking forward to generic implementations, developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before displaying it to the user.

4. Lack of Resources & Rate Limiting. Quite often, APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only can this impact the API server performance, leading to Denial of Service (DoS), but also leaves the door open to authentication flaws such as brute force.

5. Broken Function Level Authorization. Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers gain access to other users' resources and/or administrative functions.

6. Mass Assignment. Binding client provided data (e.g., JSON) to data models, without proper properties filtering based on a whitelist, usually lead to mass assignment. Either guessing objects properties, exploring other API endpoints, reading the documentation, or providing additional object properties in request payloads, allows attackers to modify object properties they are not supposed to.

7. Security Misconfiguration. Security misconfiguration is commonly a result of unsecure default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information.

8. Injection. Injection flaws, such as SQL, NoSQL, command injection, etc., occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's malicious data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

9. Improper Assets Management. APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints.

10. Insufficient Logging & Monitoring. Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems to tamper with, extract, or destroy data. Most breach studies demonstrate the time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

API Security Requirements

As exemplified by the OWASP list, the cyber security community is beginning to identify many familiar, canonical issues that emerge in the use of APIs for public-facing applications. Below are five generalized cyber security requirements for APIs that come up in design and development context frequently for both legacy and new Internet applications:

Visibility
The adage that knowledge-is-power seems appropriate when it comes to API visibility. Application developers and users need to know which APIs are being published, how and when they are updated, who is accessing them, and how are they being accessed. Understanding the scope of one's API usage is the first step toward securing them.

Access Control
API access is often loosely-controlled, which can lead to undesired exposure. Ensuring that the correct set of users has appropriate access permissions for each API is a critical security requirement that must be coordinated with enterprise identity and access management (IAM) systems.

Bot Mitigation
In some environments, as much as 90% of the respective application traffic (e.g., account login or registration, shopping cart checkout) is generated by automated bots. Understanding and managing traffic profiles, including differentiating good bots from bad ones, is necessary to prevent automated attacks without blocking legitimate traffic. Effective complementary measures include implementing whitelist, blacklist, and rate-limiting policies, as well as geo-fencing specific to use-cases and corresponding API endpoints.

API Abuse in Action

By design, APIs are stateless, assuming that the initial request and response are self-contained, holding all the information needed to complete the transaction. Making program calls to an API directly, or as part of a mobile or web application improves user experience and overall performance. This makes it very easy for a bad actor to script and automate their attack as highlighted in two examples below

Account Takeover and Romance Fraud: Zoosk is a well-known dating application. Bad actors decompiled the Zoosk app to uncover account login APIs. Using automation and attack toolkits, they then executed account takeover attacks. In some cases, compromised accounts were used to establish a personal relationship with another Zoosk user and, as the relationship blossomed, the bad actor requested money due to a sudden death or illness in the family. The unsuspecting user gave the money to the bad actor, who was never to be heard from again. Prior to implementing Cequence, romance scams at Zoosk averaged $12,000 with each occurrence. Now, they are virtually eliminated, resulting in increased user confidence and strengthened brand awareness.

Account Takeover and Financial Fraud: Another example of APIs being targeted with an automated attack involves a large financial services customer finding that attackers had targeted its mobile application login API to execute account takeovers. If successful, the bad actors could attempt to commit financial fraud by transferring funds across the Open Funds Transfer (OFX) API. OFX, of course, is the industry standard API for funds transfer within the financial services community, and as such the APIs are publicly-available and well-documented to facilitate use.

The ubiquity and stateless nature of APIs are beneficial in many ways, but they also introduce numerous challenges that traditional security technologies cannot address. By design, APIs do not have a client-side component, so traditional defense techniques like Captchas or JavaScript and mobile SDK instrumentation cannot be used elegantly to prevent an automated attack. Often, there is no corresponding browser or mobile application for redirection and cookie assignment for instrumentation. The result is that the API and associated application are left unprotected, or are protected only partially.

Vulnerability Exploit Prevention
APIs simplify attack processes by eliminating the web form or the mobile app, thus allowing a bad actor to more easily exploit a targeted vulnerability. Protecting API endpoints from business logic abuse and other vulnerability exploits is thus a key API security mitigation requirement.

Data Loss Prevention
Preventing data loss over exposed APIs for appropriately privileged users or otherwise, either due to programming errors or security control gaps, is also a critical security requirement. Many API attacks are designed specifically to gain access to critical data made available from back-end servers and systems.

The API community continues to drive toward more standardized agreement on the optimal approach to security. To this end, industry groups such as OAUTH, for example, have proposed criteria requirements for API security that are quite useful. The most likely progression is that the software security community will continue to refine its understanding and insight into the full range of API security requirements in the coming years. Observers should thus expect to see continued evolution in this area.

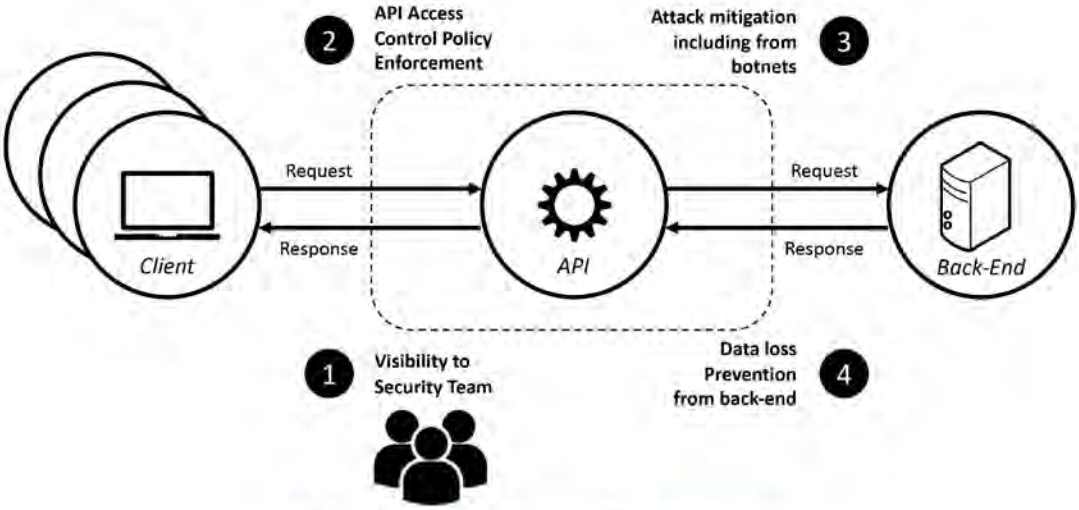


Figure 3. API Security Methods

Existing Approaches to API Security

Software developers have done their best to minimize the growing risks associated with APIs, and many useful security methods have been proposed. These methods, which are commonly found in software and application environments today, can be arranged into four distinct security solution groups (which map closely to commercial vendor types). Each group addresses specific cyber security challenges to the existing use of APIs:

- *API Gateways* – API gateways are the most mature solution category in this area. Most commercial gateways focus on visibility and control of the API processing environment.
- *API Security Offerings* – The API security market is populated with startups that locate APIs and protect them from vulnerabilities, and associated exploits such as data leakage.
- *Web Application Firewalls* – Web application firewalls (WAFs) apply in-line traditional web-based vulnerability exploit protection to APIs.
- *Access Control* – This approach, often integrated with cloud-based IAM solutions, provides policy-based mitigation for API calls based on app or workload credentials.
- *First Generation Bot Mitigation* – This method prevents automated attacks against web and mobile apps using JavaScript and mobile SDKs to collect attack telemetry.

While each of the security strategies listed above provides a degree of useful benefit, none are positioned to address all of the API security requirements listed above. As a result, software developers will often rely on multiple offerings from the mix of API security providers. This increases cost and complexity, and reduces the flexibility in the use of APIs that is so attractive, and that prompts use of APIs in application and workload management.

How Cequence Security Addresses API Security

Cequence Security Application Security Platform detects and mitigates API attacks with a container-based software platform that uses Machine Learning (ML) algorithms to identify automated bot attacks and vulnerability exploits. The Cequence platform can be deployed in the cloud, on-premise, or wherever an application is hosted, is particularly well-suited to addressing common attacks including account takeovers and API business logic abuse targeted at web, mobile, and API-based applications.

The Cequence value proposition is that it addresses gaps that currently exist in API security, with emphasis on complete visibility, , bot and vulnerability exploit prevention. Collectively, these areas are under-served in the API community, and Cequence focuses on addressing them in a manner consistent with how application developers can easily integrate the solution.

Overview of Cequence Platform

The Cequence Application Security Platform (ASP) is a commercially-available platform solution that helps enterprise security teams protect web, mobile, and API-based application infrastructure from security threats. Specific types of attacks mitigated by the Cequence platform include automated botnet attacks, and vulnerability exploits targeting applications. The Cequence protection suite uses machine learning and advanced analytics to discover applications and the attacks hiding within.

One component of the platform is called CQAI, which uses machine learning and analytics to determine the intent of application transaction, which helps to identify automated business logic abuse attacks, a commonly used attack approach targeting APIs. The CQAI findings can then be used by bot Bot Defense and App Firewall as policy enforcement components to prevent the respective attack.

The availability of commercial platform solutions such as Cequence ASP is good news for enterprise teams working with applications and APIs. Most legacy cyber security tools from commercial vendors have had a blind spot to this area, especially API security. With increases in machine-to-machine, IoT, and other automated process communications in web and mobile applications, this commercial emphasis is necessary to ensure that enterprise teams have professional support.

The Cequence platform was designed to directly address the most important of the API security requirements listed above – namely, the need for visibility, traffic management, and threat prevention. Details on how this is done are offered below.

Cequence Support for Visibility

The agentless, intelligence-based approach used by Cequence provides users with the ability to continuously monitor and build a site-map of all the APIs in use, including those accessed by users, partners, aggregators, and IoT devices. The idea of an API site-map should be attractive to application development and application security teams who would like to maintain an understanding of API access posture.

Since the Cequence platform is typically deployed at a choke-point in the application layer, it can detect and aggregate data across the entire API fabric and give a unified and real-time view of API usage to security teams. The visibility that results from such real-time operation enables users of the Cequence solution to determine and maintain an accurate security profile for the *entire* API fabric.

Using the Cequence platform, new APIs and periodic updates are automatically discovered without injecting security-caused delays into the software development lifecycle. For example, the Cequence team was able to alert the enterprise security team at a large retailer about a new version of an API application being rolled out and which was now live. That security team had been completely unaware that the problem even existed.

Cequence Support for Traffic Management

The Bot Defense and App Firewall components of the Cequence platform combine to provide high-precision traffic management based on the visibility generated by CQAI. Driven through policies, the platform can enforce a positive security model that precisely allows what users need and while denying all else.

The platform automatically detects and protects newly deployed applications to provide continuous protection. For example, a US regional bank was experiencing a burst of Open Financial Exchange transactions from East Asia, where they had virtually no customers. With the Cequence solution, they were able to divert those potentially fraudulent transactions from East Asia to an alternate server, while not impacting legitimate transactions.

Cequence Support for Threat Prevention

Experience has shown that APIs are subject to same set of cyber threats that can be executed against web applications. These threats include both automated business logic abuse and vulnerability exploits. Business logic abuse, at scale, can be driven through large automated or human bot farms, leading up to fraud and financial loss. Mitigating the effect of these threats requires preventive controls integrated with the API fabric.

As an illustration, just after the disclosure by Facebook that they had leaked nearly fifty million OAUTH tokens used for Facebook logins on other platforms, a social media customer of Cequence experienced a high-volume credential stuffing attack on their Facebook login application API. Luckily, they were able to effectively thwart that attack using the Bot Defense solution.

Public API documentation makes it easier to target API-based applications, compared to traditional web applications that require analysis, some of which is trial and error. Just like web applications, APIs are subject to vulnerability exploits to gain unauthorized access, steal sensitive data, and launch even more damaging attacks. The Bot Defense solution protects APIs from automated business logic abuse. The App Firewall prevents these APIs from being exploited by motivated and well-resourced attackers.

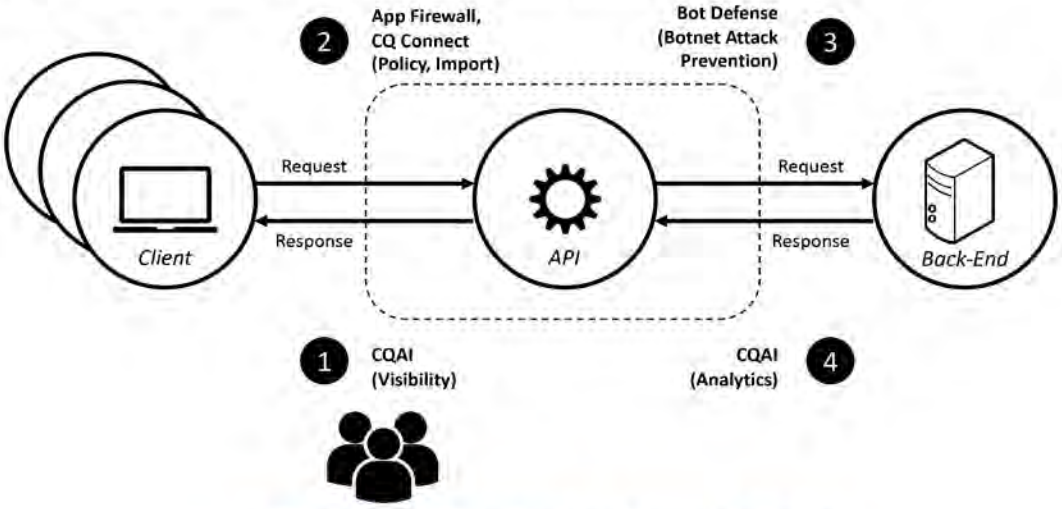


Figure 4. Cequence Platform Security

TAG CYBER

Requirements for Enterprise Security Performance Management

A set of requirements is provided for enterprise security teams to use in selecting automated platforms for their security performance management (SPM). The requirements ensure optimal integration of findings into on-going businesses processes and planning activities.

Prepared by
Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
eamoroso@tag-cyber.com

Version 1.0
April 13, 2020

Introduction

External security assessments are performed every day within organizations of all sizes, sectors, and shapes. The goals of these assessments range from identifying levels of cyber risk, to optimizing the investment being made (or not being made) in security controls. Many excellent standards provide guidance on how to perform these assessments. Methodologies are available from NIST and other capable groups to help organize internal and external reviews (see [1], for example).

More recently, however, enterprise security teams are moving away from point-in-time security assessments to related solutions that provide security performance management (SPM). These SPM engagements are continuous in nature, and include findings based on a continuous and repeating cycle of assessment, reporting, modeling, and remediating. Security assessment teams are well-suited for these on-going SPM engagements, so this might represent the future of enterprise security consulting.

As with traditional security assessments, the participants in these SPM initiatives include a variety of different actors – each with their respective objectives and biases. It is important to ensure a proper mix of actors, because the success of the SPM engagement will depend on whether this mix consideration has been made. Here are the most typical participants in an SPM project:

- *Resource Owners* – These are the teams whose systems are being assessed. These might be application owners, network administrators, business unit leads, function coordinators, system administrators, security managers, and so on. These are the groups and individuals who will have the l local responsibility to address any findings from a security assessment. They are also the ones who benefit most directly from suggested enhancements.

- *Enterprise IT and Security Teams* – The IT and security teams will generally manage the broader aspects of an SPM project and its attendant findings. For example, if shortcomings are found in the credential management for an application, then the identity and access management (IAM) team (which can existing within IT, within security, or across both) will engage directly with the application owner to improve the situation.

- *Internal Audit Team* – If important business controls are being addressed by an SPM, or if the work has implication for external regulatory or reporting requirements, then the internal audit team will often get involved. Many SPM engagements are launched at the request of an internal audit team, and a common trend is that internal auditors are becoming much more informed about cyber security technology and processes.

- *External Consultants* – It is typical for an enterprise to engage external security consultants to perform these on-going assessments. Consultants have the advantage of expertise in a given area with unbiased, independent perspectives. They can also develop expertise with complex tools for discovery, risk management, and analysis. Often, then select the platform being used for a given SPM project, including the automated stream of output reporting.

- *Executive Team* – The executive team is where final responsibility resides for addressing any findings or deficiencies from an on-going SPM. They might also be the group deciding that an assessment is required, especially if the purpose of the SPM is broad. For example, executive teams often engage security consultants to gauge the general level of effectiveness of their security program, including an independent peer comparison.

Many commercial platforms exist to help security assessment teams, internal or external, serve these important actors in the enterprise. Commercial platforms are often best used to reduce the burden of manual effort by the consulting teams. For example, gap analysis of a program against a set of security requirements was once only done using paper and pencil. Today, such work is almost always done using a governance, risk, and compliance (GRC) platform that automates the mapping process.

A challenge, however, is that the requirements used to select a good platform for SPM are often established in an ad hoc manner. Most often, the consultant selects a platform they have experience with, and the degree to which this integrates with the enterprise will range. In other cases, the assessment might use some existing tool for which the organization possesses a license. GRC platforms, for example, are often used in finance departments, so they might be reused for security.

It would be far better, obviously, for the enterprise to establish and use a set of common requirements for any on-going SPM initiatives – whether internal or external. By using commonly defined functional platform features, the stream of output from the SPM process can be optimized. Practitioners will often observe, for example, that the results of a traditional security assessment are often delivered as a thick volume that will just gather dust on some executive's shelf.

Platform Requirements for Security Performance Management

Based on the experience of the author as a practitioner consuming assessments, an expert providing on-going assessment results, and an industry analyst reviewing how assessment projects are being done, the following list of functional requirements is offered for enterprise teams interested in SPM. These requirements relate specifically to the automated platforms being used to support an SPM engagement. Obviously, for smaller projects done manually, some of these requirements might not apply.

The requirements are presented below in a manner that will make it easy to cut-and-paste into a procurement document. In fact, the style and approach used in the NIST Cybersecurity Framework Standard (800-53 Rev 5) [2] is used to help maximize consistency with the typical contract with a security consultant. Enterprise teams should also have little trouble adjusting these requirements to reflect local constraints, systems, and applications more familiar to their own project.

Control: The organization assigns [*Assignment: organization-defined personnel or roles*] responsibility to deploy and manage the security performance management platform tool used by [*Assignment: organization-defined group or individual performing the security performance management*] that addresses the following requirements:

1.1 WORKFLOW INTERATION FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Provides on-going automated integration via application programming interfaces (APIs) for all security performance management findings into the organization's preferred workflow management tools for security, including any incident response systems, trouble ticketing systems, and governance, risk, and compliance (GRC) platforms;

1.2 ANALYSIS SUPPORT FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Supports on-going automated analysis of all vulnerability and attack-related findings from the security performance management, including the ability to integrate with the organizational Security Information and Event Management (SIEM) tool, as well as to integrate with any security analytic tools for forensics, threat hunting, or endpoint security detection and response (EDR);

1.3 PLANNING TOOLS FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Supports integration of all findings from the security performance management into preferred project management and tracking platforms to ensure timely closure of all actions;

1.4 MEDIATION SUPPORT FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Provides a means for tracking, managing, and measuring the effectiveness of any security mediation activities dictated in the findings from the security performance management; and

1.5 METRICS TRACKING FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Provides support to define and track preferred metrics (including costs, staff allocation, and time) associated with the security performance management project and any subsequent actions dictated by project findings. This must include the ability to generate summary reports for executives, managers, and operational teams with the ability to flexibly tailor the metrics being reported to the needs of the group reviewing the reports.

Supplemental Guidance: These recommendations are based on the presumed availability of commercial platforms that support automated support for security performance management projects. This is a new area of the commercial cyber security community, so buyers must take time to perform the necessary research and source selection activities to locate a suitable provider.

References

[1] *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication (SP) 800-115, September 2008. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[2] *Security and Privacy Controls for Information Systems and Organizations* (Final Public Draft), NIST Special Publication (SP) 800-53 Rev. 5, March, 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

About TAG Cyber

Founded in 2016 by Dr. Edward Amoroso, former Chief Security Officer for AT&T, Manhattan-based TAG Cyber democratizes cyber security industry research and advisory through high-quality reports, guidance, and information accessible to a wide expert audience. TAG Cyber helps close the communications gap between enterprise practitioners and security vendors. TAG Cyber also offers consultation and research subscriptions for enterprise practitioners.

TAG CYBER

Cooperative Cyber Security Protection for Large-Scale Infrastructure

Prepared by

Edward Amoroso

Gen. Keith Alexander (ret.)

Part 1: Introduction

Cyber security risk has become a mainstream consideration for any organization with valued assets. This is particularly true for any group with responsibility to provide essential services, including ones that might have safety or life-critical implications if not properly managed. Power companies, financial services firms, telecommunications companies, military organizations, and government agencies all come to mind as example teams dealing with this growing risk.

What are the cyber security challenges of large-scale infrastructure?
Early computer security methods in the 1980s and 1990s were designed to address small-scale risks to systems with modest size, scope, connectivity, and scale. Early PCs, for example, were protected during these early years with anti-virus software, simple firewalls, passwords, and vulnerability scanners. While these methods do not represent the high-end of security controls in the modern era, the threat was simpler in the early days, and most observers would suggest that users felt safer during that period.

As technology expanded to the present day, and large-scale infrastructure emerged that was more dependent on computing for operation and control, the security risks grew accordingly. Unfortunately, many of the protections applied to large-scale cyber security were derived from early PC security approaches. It is not uncommon today, for example, to find a critical infrastructure security centered primarily on the use of anti-virus software, simple firewalls, passwords (sometime even non-complex or default passwords), and vulnerability scanners.

As technology expanded to the present day, and large-scale infrastructure emerged that was fully dependent on computing for operation and control, the security risks grew accordingly.

Certainly, familiar small-scale controls do play a role in the protection of larger infrastructure. Passwords and firewalls, for example, are obviously important to stop certain threats, regardless of the size of the assets being targeted. But at the same time, the unique needs of large-scale systems demand security controls that match their characteristics. Any control that requires manual handling, for example, might be fine for a small system, but impossible to manage across a massively scaled infrastructure.

Method	Small-Scale	Large-Scale
Maintenance	Manual	Automated
Visibility	Well-Known	Approximated
Assets	Simple	Complex
Configuration	Fixed	Changing

Figure 1-1. Managing Small-Scale Versus Large-Scale Systems

With these differences in mind, the owner of modern infrastructure must accept that new methods of cyber security protection are required. Furthermore, everyone knows that the simple hacker threat that drove early PC protections has been replaced by determined, capable adversaries, often funded or otherwise backed by criminal groups or nation-states. To address this type of risk, serious consideration must be given to the types of protections that are necessary to put in place to defend against the threat from such capable threat actors.

What type of protections are required for large-scale infrastructure?
To protect large-scale systems, engineers need controls that are consistent with the management considerations one finds in complex infrastructure. This implies that security controls must be fully automated; they must address the challenges of developing visibility over complicated networks; they must be designed to protect high-value assets with serious consequence if breached; and they must deal with the constantly changing nature of large-scale systems.

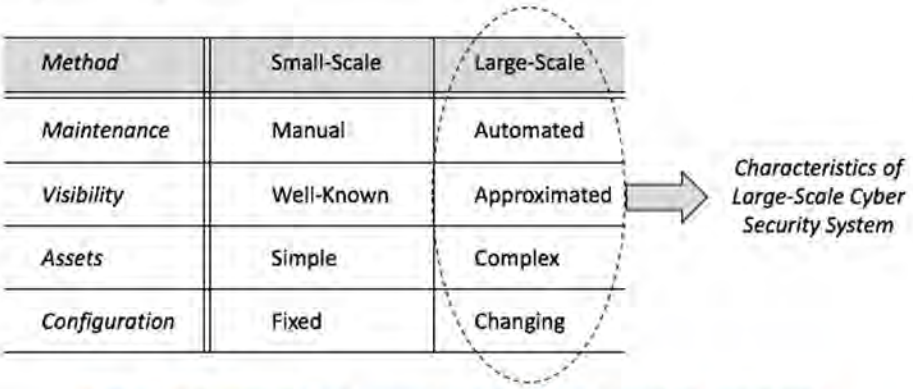


Figure 1-2. Designing Large-Scale Cyber Security Solutions

Careful planning must therefore go into the design of cyber security protection architectures for any large-scale infrastructure. Most modern Chief Information Security Officers (CISOs) in business and government recognize this challenge and now put considerable time and effort into designing and implementing their overall security architecture. But with the rising cyber threat from highly capable adversaries, individual CISO-led teams – even if they focus their efforts – will not be able to go it alone. They will often need external assistance.

Careful planning must therefore go into the design of cyber security protection architectures for any large-scale infrastructure.

Some external assistance is obvious: Businesses do not develop their own security tools, but rather buy from vendors, even in government. Similarly, information sharing groups have emerged that offer excellent means for cooperative discussions between experts (the FS-ISAC, for instance, is a great example). So, it is not controversial to suggest that business and agencies will need to work together to address cyber threats. The big question, instead, is how this objective can be best achieved.

Can different organizations agree to cooperate on cyber security objectives?
Businesses and agencies will only cooperate on joint cyber security initiatives if they see significant benefits with minimal associated risk. Admittedly, this is how almost all business decisions are made, but large-scale cyber security might be slightly different because the benefits might be less local and more holistic. That is, businesses might recognize the advantage of keeping other businesses or groups, perhaps even competitors, safe from cyber threats.

To that end, cooperation between different businesses, agencies, and other groups must address two ends of the spectrum: upside benefits and downside risks for each of the entities and groups involved. In both instances, the case can be made that, for large-scale infrastructure, both benefits and risks can cascade, perhaps even accelerating as lateral traversal of an attack occurs. That is, threats to someone else's system, however remote, might find their way to you. It is therefore worth cooperating to prevent such cascading threats.

The primary benefits of mutual cooperation across business and government for large-scale cyber defense include the following:

- *Early Warning System* – An organization can develop a much more effective early warning system if external groups share indicators in real-time. Not engaging in such sharing could limit the ability of an enterprise to capitalize on such early warning and to expose itself to the possibility that an attack to cascade locally.
- *Broader Visibility* – By working together with external groups, the local security team benefits from broader visibility, including an improved understanding of how local enterprise changes (e.g., DNS-related) might cascade to other portions of the Internet.
- *Strength in Numbers* – The simple fact that cooperation introduces more eyes on a cyber threat means that organizations that cooperate with external groups with similar capabilities are above leverage strength-in-numbers and thereby better support their local security teams.

The corresponding risks that must be managed in the development of any large-scale cooperative arrangement for cyber security include the following:

- *Privacy of Shared Data* – The possibility emerges that sharing information with a cooperative might result in leaked data or a serious privacy incident. For highly regulated industries, sharing with government may also expose businesses to some regulatory risk (although this is partially mitigated by certain provisions of the Cybersecurity Information Security Act of 2014 (CISA)) if the data is not properly anonymized or otherwise does not comply with legal requirements. Controls must be in place to ensure that cooperating teams are likewise not exposed to this risk.
- *Attribution of Incidents* – Similarly, public attribution of an embarrassing or problematic security incident to a sharing entity may reduce (or even remove) the willingness of that organization (and others) to share further information about something that might reflect poorly on their own actions.
- *Competitive Relationship* – The risk of one company directly assisting a competitor cannot be ignored, but CISA has address the key legal barriers here, and hopefully organizations will adopt the airline and energy industry's observations that a mutual focus on safety helps every participant.

The benefits and risks of a cooperative, sharing environment to support cyber security for large-scale infrastructure across heterogenous business and government groups must be used to navigate the best approach. Too often, cooperatives are developed that leave participants wondering what's in it for them and how potential problems might be avoided. It is a central thesis of this report that cooperative security arrangements will fail in the absence of suitable attention to these management concerns.

How can government coordinate with industry for cyber security?

The role of government is challenging in any large-scale cyber defensive collective for several reasons. First, most large businesses are multi-national, which suggests that while national allegiance might be easily identified (e.g., Verizon is an American company, while Huawei is a Chinese company), such allegiance will typically come second to the best interests of the company's shareholders. This emphasis is often misunderstood by government agencies who are focused exclusively on national interests but may also vary based on the typical relationships between government and private industry in various countries.

A second challenge for government is that while they can cooperate, they must also regulate and even punish organizations not meeting their security obligations – perhaps even based on innocent mistakes by employees. In cases where robust reporting is required in any event, this might not affect cooperation, but many incidents are not reportable and would thus be typically withheld from government inspection. This uncomfortable fact complicates government cooperation with business on cyber security, at least to the extent that government are permitted to regulate based on voluntarily shared information. There is a reasonable argument to be made that if governments wish to incentivize such voluntary sharing, they ought consider prohibiting regulation on the basis of shared information.

The third and perhaps biggest challenge for government in large-scale cyber security is that the majority of critical infrastructure in most countries – especially the United States – is owned and operated by the private sector. This implies that most useful telemetry, indicators, and early warnings will come from the private sector, even for many military applications and defensive government activities. This fact is often not fully understood by citizens and politicians who may demand that government step in and fix large-scale cyber security threats when the government simply doesn't have the information, nor the authority or resources to do so.

The majority of critical infrastructure in most countries – especially the United States – is owned and operated by the private sector.

In the end, a reasonable balance is required between government and industry on matters related to cyber security. Government must work hard to share information it uniquely controls, such as classified indicators that might be downgraded for sharing externally or be shared in a more limited context to defend critical infrastructure. And businesses must recognize that their obligations to society extend beyond just the shareholder, and that, in any event, it is also in their individual best interest to find way to cooperate on large-scale cyber security issues.

References

Edward Amoroso, Cyber Attacks: Protecting National Infrastructure, Elsevier Inc., 2011.

Part 2: Cyber Threats to Infrastructure

Any cooperative to support large-scale infrastructure protection must begin with an accurate perception of the real cyber risks that must be addressed. Experts understand that all forms of risk are measured by combining the probability of bad outcome with the consequences of such outcome. In the context of infrastructure protection, the risks are driven by malicious threats and consequences of compromise to valued assets. To understand cyber risk, one must understand these components.

What are the cyber threats to large-scale infrastructure?

The CIA model of confidentiality, integrity, and availability offers a well-known, textbook view of cyber threats to large-scale infrastructure. As such, it can be used to create a hierarchical representation of threats to large-scale systems. These levels of the hierarchy can be driven by general or domain-specific issues to highlight scenarios that target infrastructure assets. The depth and details of the hierarchy should always be selected to help security engineers understand threats.

The CIA model of confidentiality, integrity, and availability offers a reasonable, high-level view of cyber threats to large-scale infrastructure.

A typical hierarchical breakdown of cyber threats might be illustrated for a typical bank. The first level of hierarchical decomposition might be defined for each component business of the bank. In this case, we might assume these areas to be personal, business, loans, and investments. Obviously, these would be determined by the structure of the bank, which might vary across different banks. The resulting hierarchy, starting with CIA, and decomposing to the banking break-down, looks as shown in the diagram in Figure 3 below:

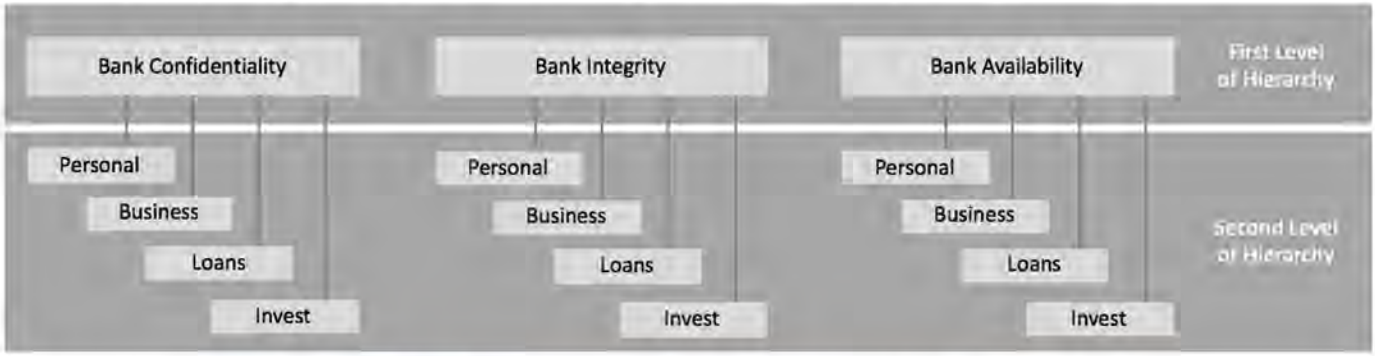


Figure 2-1. Two Levels of Hierarchical Threat Decomposition for a Typical Bank

The advantage of hierarchical threat decomposition for large-scale infrastructure is two-fold: First, the approach maintains completeness of the composite threat profile through each stepwise breakdown – so long as the decomposition is done properly. And second, the hierarchy provides detailed guidance on the specific threat scenarios that are applicable to the system of interest. Each scenario is developed by starting at the top level and working down to a leaf node.

Sample two-level threat scenarios hierarchically decomposed as part of the bank example shown above include the following:

- *Confidentiality – Loans*: This scenario might involve loan-related information being disclosed to an unauthorized individual. Such a disclosure could have serious implications for personal privacy and may result in economic harm or public consequences in a variety of circumstances.
- *Integrity – Business*: This scenario could involve business banking information being modified by an unauthorized entity. Such malicious action could undermine consumer confidence in the business and could degrade the business community's confidence in the bank or, worse, the financial sector more generally.
- *Confidentiality – Invest*: This scenario could involve the disclosure of the details of an investment, perhaps in a wealth management business, to unauthorized entities. This can be an and can introduce financial risk to the bank through litigation if disclosure resulted in material harm to the client and could be an especially uncomfortable scenario if the investor is a wealthy or prominent individual.
- Availability – *Personal*: This scenario could involve some potential malicious blocking or denial of service for personal banking customers of access to their accounts. While the immediate impact of such a scenario might seem fairly minor, the perception of or potential for a larger-scale attack could easily cause panic in populace, particularly if the outage is extended and widespread.

Every large-scale entity involved in the provision of essential critical services or assets must engage in a detailed threat breakdown along the lines of the example shown above – albeit with many more levels of decomposition. In some cases, the resulting threat hierarchy might include many thousands of leaf nodes, each corresponding to a path in the tree, and each representing one specific threat scenario that must be addressed by the security scheme.

The CIA model of confidentiality, integrity, and availability offers a reasonable, high-level view of cyber threats to large-scale infrastructure.

In some cases, it will be trivial to map scenarios from the threat tree for one organization to that of another. For example, the distributed denial of service (DDOS) threat to companies based on a botnet of compromised virtual servers will be easy to connect between different organizations. Banks, government agencies, and even the military will likely experience comparable DDOS issues and can therefore easily coordinate on an integrated response using naming, routing, and other shared attributes of potential attacks.

What are the consequences of cyber attacks on large-scale infrastructure?
The consequences of any attack on the assets of a particular infrastructure owner will obviously vary with the specific circumstances. That is, each sector of a national or critical infrastructure ecosystem may experience different consequences as the result of a hostile cyber activity. Customers of telecommunications providers, for example, may experience severe consequences as a result of even temporary service outages. Other industries, such as the fashion or entertainment profession, might not view temporary unavailability of their files as being as serious, so long as there is not an immediate impact on a particular matter.

Similarly, other contextual factors will influence the severity of consequence for threats to different large-scale infrastructure owners. For example, a large retail organization might view targeted denial of service threats just before the holiday season as having significant implications for its business. In contrast, the same retailer might view an availability attack at a different time of year, where core sales over a particular time period are less critical to the business's overall economic health, as having a significantly smaller impact. This difference matters because it also influences the measurement of risk up front.

An additional complicating factor is the fact that many organizations evaluate risk based on the measurement of so-called hard consequences, which involve concrete financial, business, and tangible asset loss, as well as soft consequences, which involve reputation and image, among other things. Regardless of the nature of the consequence, however, all organizations will have some sort of hierarchical view of their top risks, and many of these will be driven primarily by consequences – regardless of the likelihood of attack.

Organizations measure so-called hard consequences, which involve concrete financial, business, and tangible asset loss, as well as soft consequences, which involve reputation and image, among other things.

Take, for example, a pharmaceutical company that develops drugs based on years of expensive research. Theft of their medical intellectual property is often considered the top cyber risk of the company, and it is driven primarily by consequence. That is, it might be just as likely that email or calendar information for employees might be hacked. But the consequence of the IP theft is so great that it drives that particular risk to the top of the list.

Every organization managing critical infrastructure must identify their top risks. This is typically done by first listing and estimating the magnitude of the top attack scenarios based on existing vulnerabilities. The next step is to list and estimate the magnitude of the most undesirable consequences the organization might experience. Risk ranking is then done by creating a cross product of the two lists and then tuning that output into something meaningful.

An example might be a civilian agency, perhaps one that processes citizen applications for some service, that creates a list of its top three vulnerabilities. It then creates a list of the top three most undesirable consequences. Finally, it takes the cross product of the two lists, tuning the final output into an estimate of top risk scenarios that makes sense for the agency given its particular mission. Here is what such an exercise might look like for a typical agency.

Figure 2-2. Sample Risk Analysis from Vulnerability and Consequence Information

A similar evaluation for a large-scale infrastructure owner would almost certainly involve a larger and more complex list than shown in the example above. Regardless of the complexity, however, it is essential that this task be completed, as the result will help guide the internal allocation of security resources, as well as help with the evaluating individual risk in the context of a collective security arrangement. That is, even beyond assisting with direct internal security, having a strong understanding of a given company's own risks can be essential to it receiving useful assistance from its peers in a large-scale cooperative security ecosystem.

What type of bad actors must infrastructure owners focus on stopping?

Many generic taxonomies exist regarding the specific types of bad actors that an organization must contend with. These textbook descriptions of malicious entities usually include at least the following five groupings, these are not intended to be an exhaustive catalog:

Many generic taxonomies exist regarding the specific types of bad actors that an organization must contend with.

- *Hackers and Vandals* – This is the least intense group to contend with, generally because their motivation is often driven more by curiosity or reputational standing within their social group. Hackers and vandals are rarely (if ever) trying to damage society or physically harm other people, so they tend to be more easily reasoned with when caught.
- *Purpose-Driven Groups* – This is a more intense offensive group than hackers, because their attack motivation is generally driven by strong philosophical, political, or religious beliefs. This belief structure tends to result in more determined cyber threat campaigns than one finds with individual hackers. The famous hacking group Anonymous generally falls into this category of purpose-driven, malicious acting groups.
- *Business Competitors* – Although one would like to think that competitors will play fair, the reality is that in many sectors, competing organizations will aggressively seek to gain a business advantage. At times, this may result in seeking to obtain competition-sensitive information, from intellectual property data to pricing and corporate transactional information.
- *Criminal Organizations* – This group is also particularly intense and is almost always driven by financial motivation. Electronic fraud has become a popular means for stealing money, often involving social engineering front ends with robust workflow processes to execute credit card, identity, medical, insurance, and other common forms of cyber theft.
- *Nation-State Military* – As one might expect, nation-state military sponsored campaigns are the most difficult to defend against, and in many commercial scenarios, represent an intractable problem. If a nation-state such as China or Russia decides to target a business entity or to collect intelligence via cyber means, for example, then that entity is almost certain to fall victim. Given nation-state access to virtually unlimited financial and human capital, expecting individual companies to defend against serious nation-state threat actors is unrealistic given that it is truly an unfair fight in most cases.

In applying this generalized textbook categorization of threat actors, individual organizations must use their own risk analysis to determine the key malicious actors of interest to that organization. For example, an organization that scouts sports talent is highly unlikely to be targeted by a nation-state military; however, that agency would be wise to consider potential attacks from hackers and competitors as more significant threats. Such organizations may also have a broader base of threat actors — like illicit news and paparazzi groups — that might not threaten other sectors.

Despite textbook categorization, organizations must use their own risk analysis to determine the true malicious actors of interest.

What specific techniques are required to mitigate security risk in real time?
The mitigation of cyber risk is a two-fold process. First, it requires proper attention to all the security and compliance basics found in any textbook or introductory course on cyber protection. Listing this well-known litany of security policies, procedures, and functions is not necessary here. Anyone reading this report is likely to be familiar with the types of controls required in frameworks such as NIST 800-53 rev 4 or the General Data Protection Regulation (GDPR) from the European Union.

It is the extension from familiar security and compliance baselines to more advanced security solutions that are the focus of the remainder of this technical report. Specifically, we explain how the effective defense of large-scale infrastructure requires the use of a set of methods that take full advantage of analytics, data science, and network engineering methods to provide situational awareness that can drive optimal prevention, detection, and response to cyber attacks.

References

National Institute of Standards and Technology (NIST), Cybersecurity Framework, NIST 800-53 rev 4.

Part 3: Cyber Security Analytics for Large-Scale Protection

The use of certain security analytic methods and tools to protect systems from cyber threats can be uniquely suited to larger infrastructure. That is, it is unlikely that one would propose a real-time, telemetry-based monitoring system with 24/7 coverage for an individual personal computer system – unless, of course, that personal computer was connected to a much larger system or contained highly sensitive information. In contrast, however, it would be quite important to apply some sort of telemetry-based analysis capability for large-scale national or critical infrastructure protection.

What type of security telemetry is required to protect infrastructure?
First of all, telemetry is data collected by remote sensors for the purpose of improved visibility, insight, and monitoring of that target environment. Engineering issues in the integration of telemetry into a security environment include where to put sensors, how to securely pull the telemetry to a collection point, and how to tune the sensors to collect the right type and amount of data.

The type of security telemetry required to protect large-scale systems will certainly vary from one implementation to another. For instance, pure information technology (IT) ecosystems will typically generate different log information and event data than an organization that combines IT systems with operational technology (OT), perhaps in the context of industrial control or factory automation. Many OT systems, for example, use unique protocols on top of the traditional TCP/IP protocol suite.

Pure information technology (IT) ecosystems will typically generate different log information and event data than an organization that combines IT systems with operational technology (OT).

Nevertheless, requirements can be developed for the specific attributes required in any telemetry system being connected and used to protect infrastructure from attacks. The security telemetry attributes, listed below for example, will be best suited to large-scale systems, but can also be adapted and used for smaller systems:

- *Relevancy* – Telemetry collected for cyber security must be relevant to the protection goal. Event logs for systems not considered important, or activity records for networks that do not support mission-critical applications might not be relevant to the central protection task.
- *Accuracy* – The measurements inherent in collected data must accurately portray the particular system attribute being analyzed. If such measurements are crudely estimated, for example, then bad decisions could result from the interpretation of such measurements.
- *Coverage* – Telemetry for large-scale infrastructure requires coverage analysis to determine the best analytic assessment. By way of non-technical analogy, determining the current weather in the US would be poorly represented with data from one or two cities only.
- *Detail* – The data collected to support infrastructure protection must include sufficient detail to expose relevant threat issues. Event logs, for example, that only show the beginning and end of particular sessions without more detail are likely to be of limited use to security teams.
- *Attribution* – Knowing the source of data collected in large-scale infrastructure can be quite helpful in establishing context. Certainly in cases where attribution has privacy implications, caution must be exercised to ensure that such efforts are conducted consistent with the relevant legal and policy frameworks in place.

In the early days of data collection for security analytics, the general view was that the more data that is made available, the better. Most security operations center (SOC) teams today would likely disagree with this assessment and would likely argue that getting the right data from the key sources for review and analysis is the better approach. This approach minimizes unnecessary workloads and improves overall security analytic process flow in a SOC.

How can security telemetry be aggregated into useful information?

The familiar aggregation method for collected data involves sensors deployed to pull data from relevant systems of interest. These deployed sensors are tasked to create and share telemetry signals that help identify some local condition of interest. The tasking is often pre-programmed but can be adjusted both locally and remotely from a management center. Aggregated data is then shared securely with some analysis function in an analytic backend for query, analysis, and alerting. This summarized data is then provided in some user-friendly form to analysts to conduct further assessment and triage, and to take action, where appropriate. This would be supported, of course, by an analytic back-end system.

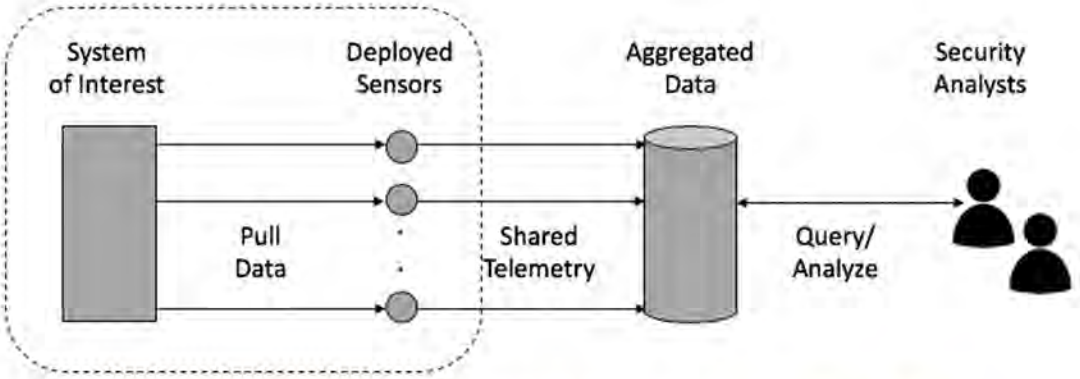


Figure 3-1. Traditional Telemetry Collection and Aggregation Method

The system of interest and the deployed sensors are most often logically or physically adjacent, whereas the aggregation and analysis function is often done remotely. This is not a rule, certainly – and some situations emerge where the relevant data or systems are not co-located with sensors — but typically these situations are resolved by routing the relevant data to the sensor through other network infrastructure products. In any event, the cadence of pulling, sharing, and analyzing data from the system, through a set of sensors into an analytic backend, and then out to an analyst in a security operations center is characteristic of any telemetry-based security protection for infrastructure.

It is worth highlighting that such detailed monitoring would likely be unnecessary for a small system, such as an individual PC as discussed above, because PCs are off-the-shelf and generally do not cause large-scale issues if hacked. Infrastructure is much harder to understand, which is why pulling data allows for approximated understanding of operation. The eminent computer scientist Edsger Dijkstra once captured the important difference between large and small systems with the following comment about an approach taken his predecessor John Von Neumann:

"[Under Van Neumann's approach,] for simple mechanisms, it is often easier to describe how they work than what they do, while for more complicated mechanisms, it is usually the other way around." E. Dijkstra

What types of algorithmic strategies are used to protect infrastructure in real time?
The specific algorithms required to identify relevant issues in collected data are generally focused on trying to predict or detect conditions that warrant security attention. Prediction occurs when the detected condition corresponds to a so-called *indication and warning (I&W)*, observed *before* some undesired consequence can occur. Obviously, I&W detection is preferred to observing an attack that has started or even completed, because in these cases, the damage might already have begun and is, therefore, harder to stop.

The overall analytic goal in the analysis of data for security is *correlation* – which involves comparison of various data looking for connections, patterns, or other relationships that connect one set of events to another. Such correlations are most usable when they are done in an automated manner, because such an approach supports rapid recognition of a condition of interest. Given the current state of the art in such correlations, however, the typical approach today is to have security analysts curating the process, with the term threat hunting emerging to describe the general process of experts guiding technology to draw fundamental security conclusions.

Three general strategies exist in the development of algorithms to support correlation between collected data and potential attack indications in a target infrastructure:

- *Signature-Matching* – This involves comparison of known patterns against observed activity. Typical signature patterns are often lists of suspicious Internet Protocol (IP) addresses or domains to be searched for in activity logs. However, these signature-based approaches can also include the type, size, location, hash values, and names of files used by an attacker, or even, in some cases, structured representations of a series of specifically denominated attack steps. The strength here is that if patterns are known, as with anti-virus software, then doing a check is a good idea. The weakness is that patterns are often unknown.
- *Behavioral Analytics* – This approach involves a more dynamic comparison of behavior patterns with observed activity. In this case, the activity being reviewed includes live operation of some system, such as whether an application is trying to establish an outside network connection or invoke some unusual operation. Behavioral analytic analysis can be more complex than signature-based review but is also more powerful in detecting indicators of attack as well as previously unknown threat vectors or attack techniques. The strength here is that signatures do not have to be known in advance, so detecting zero-day attacks becomes more tractable. The weakness is that high false positive rates can occur if profiles of expected behavior are not mature.
- *Machine Learning* – This approach involves a more advanced means for detection of cyber security threats. As a branch of artificial intelligence, machine learning tools use powerful algorithms to scan input; they make determinations based on previously processed training examples or abstractions from data they are seeing; and they establish a categorization of what has been analyzed. This approach to security threat detection is similar to how modern computers use machine learning to visualize and categorize objects. The strength here is the potential to recognize previously unknown types of attacks based on the learning process. The weakness is that the method requires an enormous amount of data. This data can be used offline for machine learning or ingested live for deep learning.

As a branch of artificial intelligence, machine learning tools use powerful algorithms to scan input; they make determinations based on previously processed training examples.

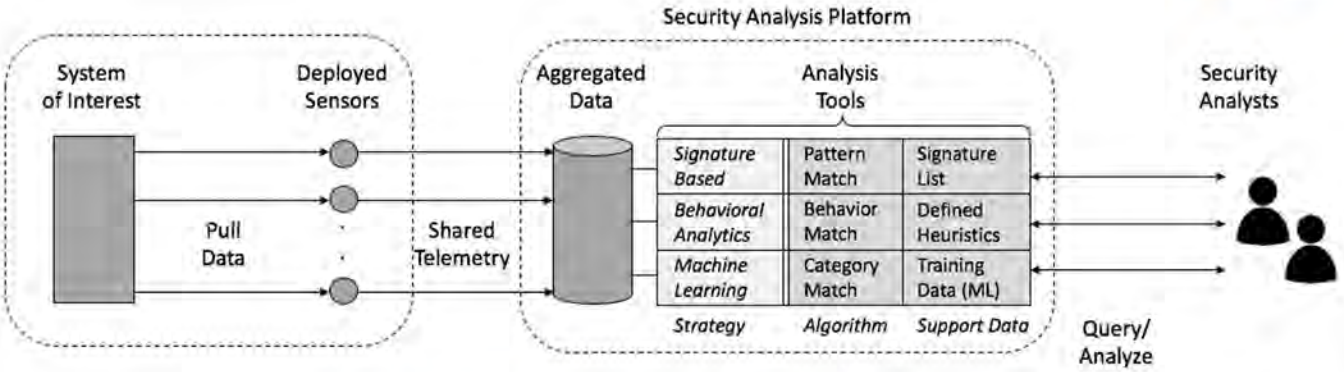


Figure 3-2. Comparing Correlation Algorithm Strategies

As depicted in Figure 3-2, platforms can certainly combine all three strategies into an effective security analysis platform for infrastructure protection. Nothing precludes the pre-processing of telemetry for known signatures, especially in cases where a rich source of intelligence is available. Similarly, if some obvious behavioral pattern exposes a malicious intent, then it is reasonable to deploy this method in advance of more powerful machine learning analysis.

Nothing precludes the pre-processing of telemetry for known signatures, especially in cases where a rich source of intelligence is available. Similarly, if some obvious behavioral pattern exposes a malicious intent, then it is reasonable to deploy this method in advance of more powerful machine learning analysis.

Is it possible for organizations to work together to reduce risk?
In general, organizations within the same industry sector or across key critical sectors will have comparable threat issues. This suggests a mutual interest in working together to share data to improve identification of both known and emerging threats. A reasonable heuristic for such processing is that having more relevant data improves establishment of data relationships. So, it should be a goal for any team protecting critical infrastructure to try to work with peer groups in the same industry.

There are serious challenges, however, for organizations to cooperate and share data to reduce their mutual cyber security risk:

- *Competition* – The competitive forces between organizations might cause them to question whether cooperation is in their mutual best interests. Certainly, some industries will naturally gravitate toward a coordinated approach (e.g., airlines agreeing to cooperate on safety issues). But other industries might include participants who benefit when their competitor is breached (e.g., retail, telecommunications, and sometimes even banking).
- *Attribution* – If shared information can be easily attributed to a reporting source, then cases emerge where this can be used to embarrass the source, or even influence customer behavior. Full anonymity options are thus essential in any information sharing initiative designed to support cooperative cyber protection.
- *Liability* – This emerges in cases where the legal implications of an incident might be unknown or still under consideration. Obviously, regulated organizations must report their incidents, but in the earliest stages of an incident, reporting obligation might not be known, and the tendency will be to hold off on sharing until the legal and liability posture of an incident are understood.

None of these challenges are insurmountable, but all require careful attention if the goal is to create a cooperative protection solution for multiple infrastructure organizations. In the next section of this report, we will examine how one vendor – IronNet Cybersecurity – has constructed a platform that not only serves the technical needs of a SOC team for correlating telemetry, but that also addresses these operational challenges for reporting organizations.

Part 4: The IronDome Approach to Infrastructure Protection

Co-founded in 2016 by General Keith Alexander, former Director of the US National Security Agency (NSA) and Commander of the United States Cyber Command, IronNet Cybersecurity focuses on advanced behavioral threat detection for enterprise networks. IronNet uses advanced analytics and sensors that pull data from defined locations in an enterprise and provides alerts that are culled in an automated manner.

The IronNet system integrates the knowledge and capabilities of its highly skilled cyber threat analysts that previously conducted offensive and defensive operations in support of national security missions. The system also shares data from multiple enterprises and industries in real time to create a collective defense fabric at scale. The company, which supports business and government customers across all sectors, serves as an exceptional case study to understand large-scale infrastructure protection.

How does IronNet's platform work?

The platform for supporting data collection and analytics to serve the cyber threat hunter is called IronDefense. Telemetry is collected from IronDefense sensors that are deployed across the enterprise at key locations to collect full packet capture (PCAP), which is then analyzed for key potential threat attributes and combined with collected metadata to create highly enriched metadata, known as IronFlows, which are then presented for analysis to the platform backend.

The CIA model of confidentiality, integrity, and availability offers a reasonable, high-level view of cyber threats to large-scale infrastructure.

The back end directly serves the threat hunter, who might choose to integrate the IronNet metadata with other telemetry and data analytics on a complementary platform in the SOC. The back end also provides event information to be rendered into the IronVue analyst front end. In addition, the back end analysis presented in IronVue can be used to coordinate detection, prevention, and response activities with peers through the IronDome collective defense platform.

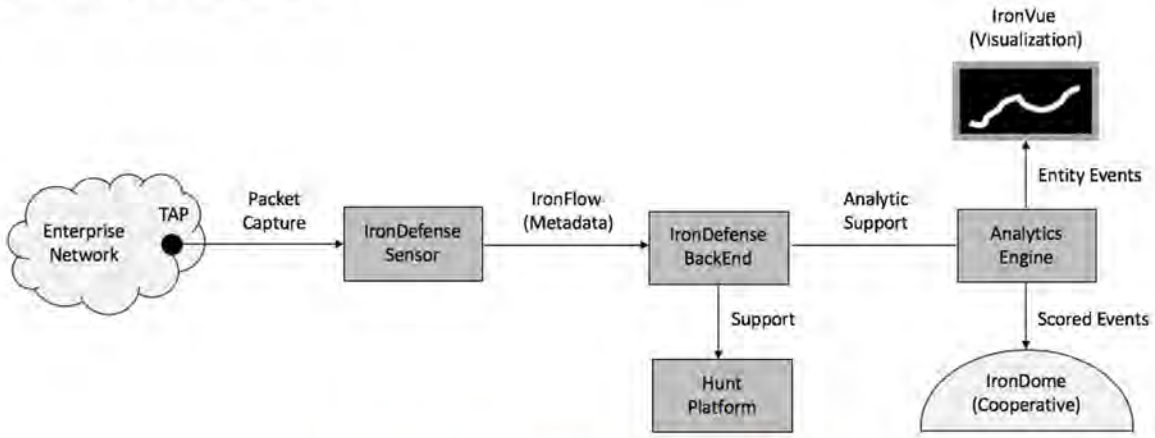


Figure 4-1. IronDefense Processing Flow

The IronDefense processing flow includes functional components required to translate raw network data into actionable intelligence. This, ultimately, is the overarching goal of any live defensive protection system for large-scale infrastructure. A key design objective in any such system is to minimize the time between collection and interpretation and to simplify each of the interfaces, ensuring an open design so that third-party systems, such as hunt platforms, can be easily integrated into the process flow.

The IronDefense processing flow includes functional components required to translate raw network data into actionable intelligence.

What functions are supported by the IronDefense analytics engine?
The analytics component included in the IronDefense platform supports the following real-time functional and process objectives for the SOC team:

- *Advanced Behavioral Analytics* – The behavioral analytics used by the IronNet system are driven by predictive behavioral models developed by IronNet data scientists supported by US government and academic research centers.
- *Driving Key Decisions* – An expert system is included to conduct contextual data analysis based on tradecraft insights and risk determinations that would typically be made by human analysts in a SOC and leveraging the core insights of IronNet's team of hunters and their prior offensive and defensive national security experience.
- *Focusing Detection Priorities* – The IronNet expert system provides useful context to any mathematics-only solution, because while a true-positive might be detected, it might not be of local interest. Adware attacks, for example, might produce a positive detection, but might not be a high priority to the local team.
- *Support for Hunt* – The SOC hunter's investigative case work utilizes the collected data in a tool that provides rapid, easy access to packet-level data and other contextual information.

Some of the major functional advantages of an analytics-rich processing environment include detection of threats at scale, which is important for infrastructure, where visibility and identification of otherwise unknown threats can be a challenge. Collection of data from key north-south and east-west collection points expands this visibility aperture and enables better response. The tradecraft insights embedded in the behavioral algorithms also help ensure that good mitigation and response decisions are made.

How does IronDome collective defense work?
The purpose of IronNet's IronDome collective defense platform is to create and support a cooperative cyber defensive system based on the live sharing of anomaly and event information for members. The collective group is built from willing peers, presumably enterprise and government organizations, who understand the need to belong to a trusted group that can expand the attack visibility surface beyond their own perimeters and enterprise networks.

The purpose of IronNet's IronDome collective defense platform is to create and support a cooperative cyber defensive system.

One advantage of this arrangement is faster time-to-detection rate for a member and the identification of threats that might have gone unnoticed in a single environment. In addition, members avoid the challenge of working in isolation against a nation-state adversary that focuses on leveraging similar offensive playbooks against a sector. The collective defense addresses this asymmetry. Here is the normal detection time for an enterprise, usually about 100 days from breach to awareness:

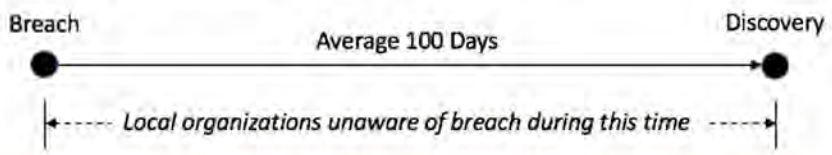


Figure 4-2. Breach Detection Time for an Organization in Isolation

When a SOC team has access to detection flow information from multiple enterprise teams in a collective such as IronDome, the potential emerges that threat warnings arrive much more quickly. If two organizations are vulnerable to some breach X, then the possibility arises that one might detect it more quickly and can notify the other. The result is a reduction in time-to-detection for the organization being notified, as shown below:

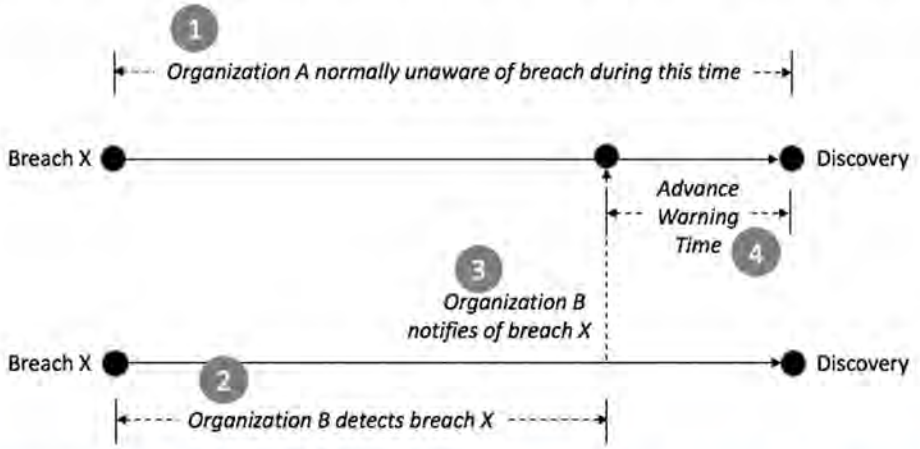


Figure 4-2. Reducing Breach Detection Time Through Cooperative Notification

The advantages of such cooperation should be obvious, and the IronDome infrastructure is set up to support this type of mutual sharing. It includes mechanisms to support the following important goals for cooperative cyber defense:

- *Industry-Wide Threat Visibility* – This aspect of IronDome solution provides participants to obtain shared event summaries with analytics for security awareness and threat insights across communities that have comparable risk profiles.
- *Community Triage* – IronDome leverages shared insights to detect broad or targeted campaigns that would not be easily detected by a participant in isolation. This aggregation capability can also work across different sectors or risk profiles.
- *Automated Machine-Speed Sharing* – IronDome automatically shares sector-based threat insights from participants and supports the maintenance of near-real-time threat analysis about cyber security issues being observed.
- *Cross Sector Defense* – Ultimately, IronDome supports a cross-sector defense for participants through exchanges across different industries, regions, and even national organizations. The result is a powerfully woven, integrated cyber defense.

These capabilities obviously rely on shareable events being passed securely and anonymously to the IronNet Cloud, where the engine and analytics store and process the information. Feedback is then shared with an IronDome of different companies, which is essentially a trusted collective that benefits from the scored events, correlations, notifications, and suspicious behavioral reports provided by the IronNet engine.

Are there any hurdles to developing a large-scale IronDome solution?
The greatest hurdle to large-scale collective protection via IronDome is that many organizations have a long-held, built-in hesitation to share threat and vulnerability information externally. This is a reasonable concern, because capable adversaries covet knowledge of IT infrastructure, network design, deployed applications, and security architectures in designing a targeted offensive. Information sharing can expose this data to external entities and might cascade to an adversary.

The greatest hurdle to large-scale collective protection via IronDome is that many organizations have a long-held, built-in hesitation to share threat and vulnerability information externally.

The design goals that can minimize information sharing concerns amongst participants include the following requirements:

- *Participant Anonymity* – When a participant shares vulnerability information with a group, the attribution should be sufficient to provide context around the shared item but should include nothing more. This implies that casual marking of a shared vulnerability with its originator is not a desired practice and could easily undermine the establishment of effective sharing. Anonymity must be embedded in the sharing infrastructure, presumably using encryption or blinding as part of the protocol.
- *Secure Storage* – The means for storing shared vulnerabilities must be trusted to be highly secure. If external, untrusted actors find their way into shared databases, then this can represent an undesirable leak, and can also undermine the trusted group. Secure storage techniques must therefore be in place, and this would presumably include best-in-class cyber security functions, procedures, and policies.
- *Trusted Groups* – The community for sharing should involve a group of participants who are mutually trusted to handle information, maintain discretion, share sufficient information to balance what is ingested, and to be a helpful partner should unexpected challenges emerge in the context of sharing (such as during an incident). Trusted groups are easier to develop when small, but context increases with the size of the group. A proper balance should be desired.

The IronDome solution includes support for these important requirements, and embeds the associated functional support directly into the platform. It should be obvious, however, that despite any functional measure put in place, the most important aspect of any cooperative, collective cyber defense is the mutual trust that exists between participants. For this reason, great care must be taken when selecting teams to include in a sharing group – whether within a sector, or across multiple ones.

Part 5: Developing Your Own Infrastructure Protection Solution

The era of government protecting business and citizenry from serious attacks including from foreign adversaries might be viewed as having passed – at least in the context of cyber security. That is, while it remains reasonable to expect government to ensure that physical attacks such as from bombs and missiles are prevented, it is sadly neither correct nor reasonable to expect any nation's military, regardless of its ability, to stop major cyber threats from hitting its citizenry and business community.

It is sadly neither correct nor reasonable to expect any nation's military, regardless of its ability, to stop major cyber threats from hitting its citizenry and business community

As a result, every organization must develop its own plan and associated solution for infrastructure protection. The good news is that this plan and solution can be constructed using existing enterprise security programs as a base. That is, the types of functional, procedural, and policy decisions made to stop enterprise-grade threats represent the correct underlying security base on which to build a foundational model for dealing with larger threats.

What attributes must be present for organizations to succeed in a cooperative?
Three attributes must be met by an organization before cyber risks to critical infrastructure can be properly addressed via a cooperative sharing group. These attributes line up directly with the belief structure of the stakeholders and decision makers in the information technology, infrastructure, and cyber security groups. These are not attributes that can simply be imposed on an organization. Rather, they must be closely held by the relevant principals:

- *Risk Acknowledgement* – An organization acknowledges security risk to their infrastructure. If the belief exists that vulnerabilities are minor and that infrastructure cannot be seriously degraded via cyber threats, then participation in a cooperative group would likely not be successful. Organizations must be willing to acknowledge the presence of risk before joining any collective sharing group.
- *Willingness to Share* – An organization must also recognize the bidirectional nature of information sharing. That is, joining a cooperative cannot be done to collect data from others. Rather, just like in any trusting relationship, it must include an open willingness to share information with other members of the group. Anonymous, non-attribution can be helpful, but willingness to share is essential.
- *Desire to Mitigate* – The purpose of any cooperative sharing group is to provide a rich source of information, from which actionable intelligence can be derived. Involvement in the group should therefore be predicated on the desire to actually mitigate cyber security risk, rather than to meet some compliance obligation, or to collect interesting information for the entertainment of the board.

Figure 5-1. Three Attributes Required to Succeed in a Cooperative

These three conditions must be met honestly by the organization, and are listed here to help make the collective involvement successful. Any organization that doesn't fully accept the presence of cyber risk, doesn't plan on sharing relevant information with others, and has no intention to use the shared data as the basis for real security mitigation and response would be advised to invest their time and efforts into other types of management activity.

It is worth mentioning that some organizations like to be part of information sharing groups to collect information relevant to executive and board presentations. Board members, in particular, like to be provided context around cyber threats, including malicious actor attribution, so sharing often helps to obtain this information. So long as the ultimate purpose in educating board members is to improve the overall security posture of the organization, this motivation for joining a collective seems acceptable.

What are the parameters for establishing trust in a cooperative?

The concept of trust between participants in any cyber cooperative is influenced by a couple of factors. First, there is the business or government sector between participants. It is not a stretch to assume that participants in a common sector will tend to be more trusting of information being ingested, simply because the vantage point will be similar. Two banks, for example, will tend to trust their relative interpretations of some vulnerability and its consequence.

It is not a stretch to assume that participants in a common sector will tend to be more trusting of information being ingested, simply because the vantage point will be similar.

Second, the relative size of sharing participants will influence mutual trust. A general rule is that most organizations will tend to trust information from larger or peer groups, but will be more tentative about information coming from a smaller participant. This is not a perfect correlation, because a large bank might trust information coming from a tiny, but expert advisory group. In general, though, peer or larger organizations tend to be assigned more confidence in the information being shared.

These two factors – sector and size – can be merged into a so-called measure of peer *correlation* that can be useful in analyzing the potential effectiveness of a given cooperative. By creating a simple grid on these two factors, we can depict the degree to which participants will tend to view the level of correlation for information being shared generally. Two large banks, for example, might find some shared data highly correlative, whereas a small retail shop might find the same data less applicable.

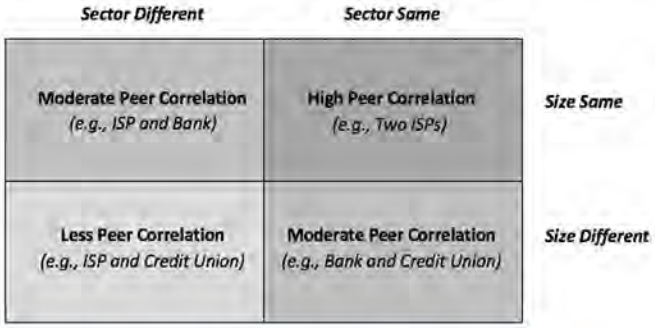


Figure 5-2. Peer Correlation in a Cyber Cooperative

It is worth noting that competitive forces will clearly influence the willingness of a given organization to share information with a cooperative group. While it is true that many industries such as transportation and energy tend to not differentiate based on relative security capability, there are some industries such as telecommunications where this is not true. Cooperatives that include entities competing on cyber-related capability will have to work harder to maintain mutual trust.

Are there any legal or privacy issues associated with joining a trusted sharing group?
Joining an information sharing group will introduce myriad management questions from the legal and privacy teams in any organization, especially larger ones with more attack consequence. These questions are best addressed before the decision has been made to join a sharing group, so as to avoid the costs of unraveling entry. The biggest issues that tend to require consideration when joining any cyber security cooperative are the following:

- *Protecting Information* – By sharing information with a cooperative, the organization introduces the possibility, however potentially small, that sensitive data will be mishandled and leaked. To deal with this issue, cooperatives must include world-class mechanisms for protecting and handling data both in storage and at rest. Participants should have influence on how these privacy and security mechanisms are selected and managed to maximize comfort levels.
- *Working with Competitors* – If a cooperative includes competitors, then legal teams will want a clear understanding of all policies and procedures used for interaction and sharing, especially in industries that are government regulated. The primary concern is that the sharing should never create cooperative marketing or pricing advantages for sharing participants, or any other business practice considered illegal or unethical. Legal teams will want documented evidence of how this all works.
- *Avoiding Unexpected Risk* – In general, enterprise legal, privacy, and security teams will be averse to any unexpected risk that might emerge as a result of joining a sharing cooperative. This requires that cooperative cyber sharing groups must include clear documentation of the experiences and expectations for all participants. New risks can always emerge, but surprise should be minimized.

In general, enterprise legal, privacy, and security teams will be averse to any unexpected risk that might emerge as a result of joining a sharing cooperative.

The best way to handle these legal and privacy issues is to directly involve staff from these organizations into the decision-making process around joining or establishing a group. Companies such as IronNet Cybersecurity can provide excellent advice to companies considering use of cooperative such as their IronDome, and can help legal, policy, and privacy staff become more knowledgeable and comfortable around what to expect.

How can I learn more about the IronNet and IronDome solutions?
Readers interested in learning more about how IronNet Cybersecurity can help them either join or establish a cooperative cyber threat information sharing group via the IronDome solution, should contact ABC XYZ at abc.xyz@ironnetcybersecurity.com and a discussion can be set up. Companies of all sizes and from all sectors have begun to benefit from this cooperative support, and with malicious threats to critical infrastructure continuing to escalate, no time is better than the present to take action.

TAG CYBER

Adding Continuous Security Validation to NIST 800-53

Continuous security validation (CSV) provides high assurance that enterprise security controls are operating as expected through ongoing test and attack simulation. Since existing security compliance frameworks do not directly reference CSV, organizations might miss the unique advantages of CSV in their compliance work. To address this gap, CSV-related language is proposed here to augment the NIST Cybersecurity Framework.

Prepared by
Dr. Edward G. Amoroso
CEO, TAG Cyber and Research Professor, NYU
eamoroso@tag-cyber.com

Introduction

Cyber risk management frameworks have a significant influence on protection decisions in the enterprise. Frameworks, such as the NIST Cybersecurity Framework [1], help organizations define how cyber security controls should be applied in practice. What they cannot do, however, is show organizations how to deploy and operate the actual systems that implement these controls. To do this properly, security teams must truly understand their business.

Unfortunately, many teams do *not* understand their business well enough to deploy controls with comprehensive coverage. In fact, this may be the toughest challenge in enterprise security today – namely, the connecting of security systems to the correct business functions to protect the right assets. Enterprise security is thus a complicated task and requires the best available support mechanisms to optimize information risk management.

An additional consideration is that security is presumed to be continuous in the enterprise. A next-generation firewall, for example, is expected to work post-deployment with no protection gaps. This is partially true for controls like vulnerability scanning but not true for periodic validation controls such as testing or simulation. These are typically not done in a continuous manner, which can reduce their effectiveness, especially given the rapidly changing operating dynamics of modern enterprise.

To address these challenges, most organizations have two teams: One focused on compliance and another focused on security. In the worst case, these two teams work separately with little coordination. In the best case, the compliance work is intended as a control check on the operational security ecosystem. In all cases, the control checking *should* be continuous – but nearly all modern compliance programs include only periodic tasks, sometimes with annual gaps in coverage.

It is therefore imperative that security teams close such gaps with mechanisms that complement control checking by compliance teams and which can validate that security operations functions are working as expected. CSV provides exactly this type of enhancement. Designed to address the weaknesses of point-in-time security investigation, CSV is a new branch of cyber security with great promise.

Specifically, CSV ensures that enterprise security organizations do not assume operating risk through relaxation of preventive security functions. Using ongoing monitoring, teams can ensure that controls are being properly facilitated by security operations. The greatest advantage of CSV is that security teams will know quickly if the effectiveness of a given security control has failed, and this can help throughout all relevant lifecycles, including the SDLC.

In this note, we recommend adding CSV requirements to security compliance frameworks, and the NIST Cybersecurity Framework, in particular. Such improvement to the framework is intended to help bridge the control validation gap between security and compliance teams through more common review goals, and through improved assurance that security mechanisms are working properly. We include language consistent with the NIST approach so that cut-and-paste enhancement is possible.

Continuous Security Validation Overview

Implementation of CSV involves use of a platform that continually simulates, tests, and validates cyber security functions across the enterprise. This is best done in the context of an adversarial threat model (the MITRE ATT&ACK Framework is a representative taxonomy [2]). The enterprise benefits from such ongoing assessment of weaknesses with respect to a known, relevant attack model. This results in an improved understanding of which security techniques are most relevant to the organization.

In contrast to CSV, point-in-time approaches include maturity assessments, independent audits, penetration tests, bug bounty programs, and functional testing. While these are important tasks, and should be part of any program, they exhibit the core weakness that any instantaneous validation test would exhibit. That is, once any test has been completed, it validates a given property at that time and limited only to the scope of the test. Subsequent changes might easily invalidate the test.

CSV addresses this weakness by reducing the interval between simulations. If implemented well, attack emulations (which can be on-premises, across virtual private clouds, and over multi-cloud architectures) can provide assurance about required control correctness (or incorrectness if a test so determines). Once CSV has been integrated into the enterprise, its results can be combined with risk governance, operational change management, software lifecycles, and other enterprise business processes.

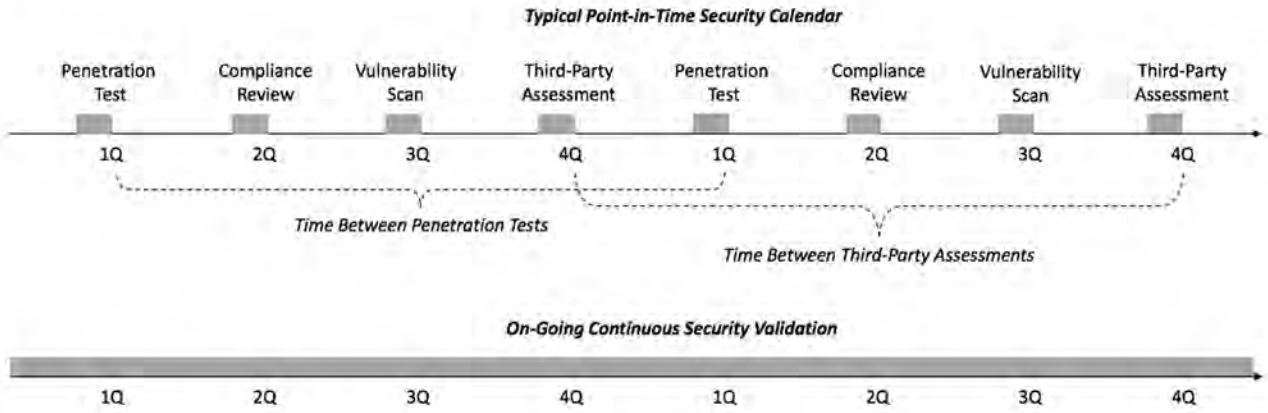


Figure 1. Comparing Point-in-Time to CSV

One obvious advantage of CSV is this reduction in time gaps between subsequent security validations. The comparison in Figure 1 shows the typical durations that exist between subsequent penetration tests, compliance reviews, vulnerability scans, and third-party assessments. Because CSV includes automated testing, adversarial emulation, and stressing of the applicable controls, it closes these gaps and provides a superior form of assurance.

An additional important advantage of CSV for the enterprise is its function in providing assurance that existing controls, including ones demanded by compliance frameworks, are operating as expected. Without this type of continuous assurance, it is likely that despite the effort to demonstrate compliance with NIST or similar frameworks, the required protections might be operating in a degraded manner. CSV addresses this potential weakness.

Adding CSV to Security Frameworks

Security frameworks offer an incentive, non-optional in regulated industries, for organizations to perform security properly. Unfortunately, as we've explained above, the temporal requirements that address audits, sampling, and periodic tests fail to provide sufficient periodicity and efficacy. A lot can change in an enterprise between audits and tests, and CSV directly addresses this gap. It is therefore valuable to include continuous and improved efficacy constructs in compliance frameworks.

Perhaps because CSV is a new form of assurance delivery, the most popular cyber security frameworks in use today do not include direct mention of this functionality. Certainly, the use of CSV will directly or indirectly touch on many of the applicable controls one is likely to find in a given framework. The Risk Assessment (RA) and System and Information Integrity (SII) families of NIST 800-53 include many requirements that are adjacent to the activities involved in CSV.

What is missing, however – and what would be particularly helpful to compliance managers, enterprise security professionals, regulators, and other stakeholders in enterprise information security – is compliance framework language that can be directly appended to the existing control language. In the section below, we provide just that: We write CSV requirements in the language and format of the NIST Cybersecurity Framework (NIST 800-53).

Our presumption is that enterprise teams might use this additional compliance requirement to augment their existing control framework. They might also use our language to future-proof their existing compliance and assurance program, since it seems inevitable that CSV will be added eventually to most frameworks. In addition, we hope this proposed addition is considered by the purveyors of popular security frameworks. We believe CSV language would be a valuable addition.

Regulators, in particular, should consider amending or augmenting their security risk management frameworks to include CSV. The goal should be a more continuous and comprehensive approach to control validation and reporting with outcomes tested in an ongoing feedback loop. Recommendations can be included as to how and where such control validation is done, perhaps with higher assets being tested more frequently.

NIST Framework Requirements

For NIST 800-53 (currently working toward revision 5), the proposal here is that a new control CA-10 be defined called Continuous Simulation and Validation. This new entry can be included in the "Security Controls to Achieve Enhanced Assurance," and complements many existing controls in the framework. It does, however, provide support for a new breach and simulation function that is not required currently in the criteria. Below is the proposed draft write-up:

CA 10 CONTINUOUS SIMULATION AND VALIDATION

Control: The organization assigns [*Assignment: organization-defined personnel or roles*] responsibility to deploy and manage a continuous simulation and validation tool that

a. Provides ongoing validation of effectiveness of the deployed security functions and controls in the organizational security architecture;
b. Performs ongoing automated simulation of attacks based on an [*Assignment: organization-defined breach and attack framework*];
c. Minimizes frequency of continuous validation to [*Assignment: organization-defined frequency of validation*].

Supplemental Guidance: This control is based on an enterprise cyber security method known as breach and attack simulation (BAS) where automation is used to simulate, test, and validate the effectiveness of deployed control. Such automation is typically driven by a comprehensive breach framework that includes a meaningful taxonomy of attacks based on practical observation of cyber threats. The MITRE ATT&CK taxonomy is an example of such a framework.

Control Enhancements: None.
References: NIST Special Publications 800-12, 800-100
Priority and Baseline Allocation:

P1	LOW CA-10	MOD CA-10	HIGH CA-10

TAG CYBER

Managing PC Firmware Health for Enterprise IT Cost Reduction

By establishing a program to systematically manage the firmware health of PCs in an enterprise, meaningful cost reductions can be obtained by extending replacement intervals.

Prepared by
Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
eamoroso@tag-cyber.com

Version 3.0
July 8, 2020

Introduction

Technologists often joke that for any new capability request, a choice must be made. That is, if you want more features, faster delivery, and reduced cost, then accept that you can only have two of the three. If you pick faster and cheaper, for example, then expect fewer features; if you pick more features delivered more quickly, then expect to pay more; and so on. This is a familiar aphorism, but it seems to accurately describe many practical situations.

Luckily, all three objectives *can* be met in certain cases where the conditions are just right. One might argue, for example, that Amazon seems to provide the most features delivered at the fastest pace at the lowest cost. So the goal of obtaining all three objectives is not impossible, but is rather quite difficult. As analysts at TAG Cyber, we are therefore always on the watch for such cases, because when they emerge, the implications can be exciting.

During the course of our day-to-day strategic discussions with enterprise security teams and commercial cyber security vendors, a creative idea related to device firmware emerged that seemed to exhibit all of these attributes. Specifically, we have observed that explicit, on-going programs focused on device firmware health can be used by IT and security operations staff to reduce cyber threats, but also to extend the useful life of deployed PCs.

Specifically, we have seen that enterprise teams can establish a review program of device firmware health for PCs, which can improve the integrity and safe operation of these devices. What is most interesting, however, is the potential cost saving that can come from *increases in normal PC replacement intervals*. These extended intervals can be estimated and calculated into truly meaningful cost improvements – hence this report.

Establishing PC Health

Enterprise IT and security teams know that modern laptop computers are built from a large number of underlying functional components, many of which are dependent on firmware for their correct operation. This implies that the integrity of the firmware for these component entities plays a large role, along with the higher-level system software, in determining the collective integrity of the system.

This is an often-missed observation by enterprise IT and security teams, because the continued integrity and usefulness of a given PC will typically be determined by factors that do not include firmware health. Instead, PC replacement is more commonly driven by causes such as physical wear and tear, increases in reported failures for the device, and intangible influences such as employee desire to be issued new devices with more modern features.

Despite this blind spot for many organizations, clear guidance is available on how PC hardware failures are often the result of firmware troubles. HPE recently issued a warning, for example, that a specific firmware patch can prevent premature PC failure[1]. Lenovo issued a similar warning that improperly patched firmware could lead to PC users experiencing symptoms such as ports not working and batteries not charging[2].

In general, the replacement period for PCs will be determined by calculating the impact of considered factors from the time of issuance to the employee, to the time of recommended replacement. What happens is that the impact of wear and tear, functional degradation, and other factors reaches a collective threshold beyond which the employee is viewed to be better off with a new PC (see Figure 1).

[1] https://www.zdnet.com/article/hpe-tells-users-to-patch-ssds-to-prevent-failure-after-32768-hours-of-operation/

[2] https://pcsupport.lenovo.com/ca/en/solutions/ht508988/

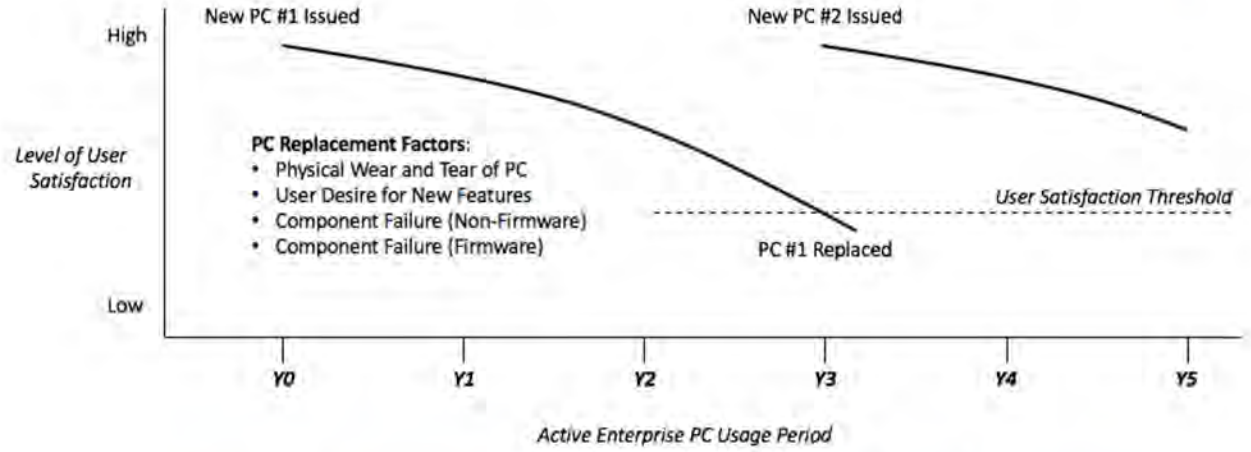


Figure 1. Typical PC Replacement Period and Factors

A typical PC replacement interval for an enterprise might be roughly 3 years, although some organizations might tend to have shorter periods, especially if new features such as increased CPU speed directly influence productivity. Software developers, for example, will be issued new devices more frequently than employees where new PC features are less essential to support every day activity (e.g., sales professionals, clerical workers).

Cost Savings Analysis

PC replacement intervals are typically not pre-determined, but rather arise from the day-to-day experiences and observations of the IT operations team. Some organizations wait for employees to report PC problems before initiating replacement, but this passive approach has the great disadvantage of ensuring that every user will eventually experience PC maintenance problems and the associated negative impacts.

So, it is more frequently the case that IT operations teams will arrive at PC replacement intervals that minimize maintenance and user inconvenience costs, but that also maximize the usefulness of the issued device. This can change over time, such as if employees are reporting problems with their PCs sooner than the average replacement time. If this happens, then the IT operations team will plan and budget to replace PCs more quickly on average.

This can also go the other way, where employees have longer periods of usefulness for their PCs than has been estimated. Where some replacement factors cannot be easily fixed by addressing uncontrollable issues such as the normal wear and tear on a device, other factors can be managed. Firmware health is one of the more promising such factors, because commercial tools exist that can ensure help ensure device integrity.

Some common methods used to protect devices at the firmware level include assurance of timely firmware patching, management of all firmware updates, testing of all approved firmware changes, guidance of firmware upgrades, stewardship of user practices during firmware update operations (such as unplugging during an update), and use of firmware signing practices with strong public key cryptographic means.

If these practices are put in place at the enterprise, then it is conceivable that the PC replacement interval will increase by reducing the number of firmware-related causes for users becoming unhappy with their devices. Obviously, this increased interval will vary based on the conditions and characteristics of the local IT operations team. This effect is shown in the conceptual graph of Figure 2 below.

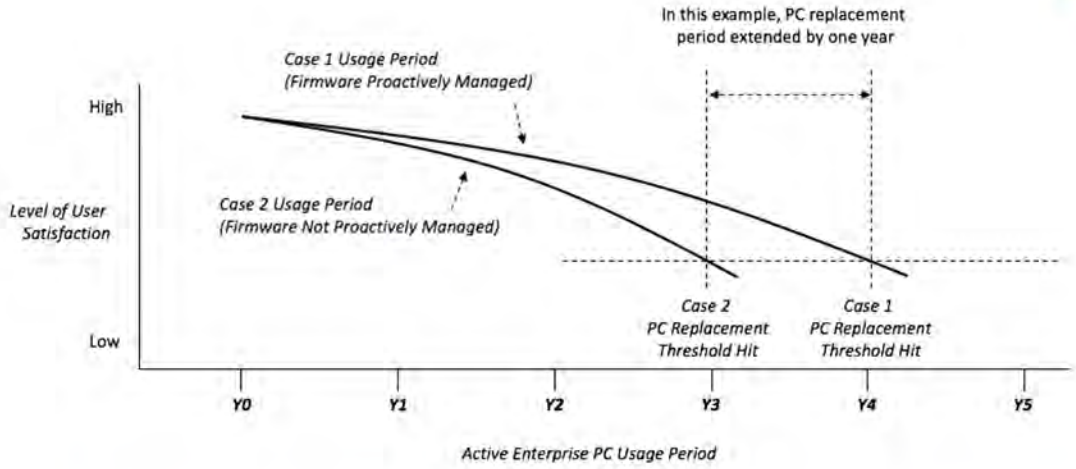


Figure 2. Managing Firmware to Increase PC Replacement Intervals

It is possible to create a simple cost savings analysis for PC replacement based on the conceptual firmware integrity management model. Assuming that PC replacement costs average between $400 and $1500 per device[3], and that device deployments range from 1000 to 10,000 devices, we can calculate possible annual cost savings of extending replacement interval. The table below shows some sample numbers.

Replacement Cost Per PC	Number of Deployed PCs	Replacement Period Increase	Annual Cost Savings
$400	1000	0.5 year	**$200K**
$400	10000	0.5 year	**$2.0M**
$400	1000	1.0 year	**$400K**
$400	10000	1.0 year	**$4.0M**
$1500	1000	0.5 year	**$0.75M**
$1500	10000	0.5 year	**$7.5M**
$1500	1000	1.0 year	**$1.5M**
$1500	10000	1.0 year	**$15M**

Figure 3. Summary of Annual Cost Savings by Increasing PC Replacement Intervals

The implication of this analysis is that enterprise teams would be wise to consider a program of firmware health monitoring and improvement. There are obvious security advantages to such initiatives, independent of the PC replacement savings described here. Excellent platforms and tools exist to assist with firmware integrity from vendors such as Eclypsium, so enterprise teams should have no trouble achieving this goal with an excellent commercial partner.

[3] Several resources on the Internet suggest replacement costs of between $400 and $3500 for PCs and laptops. (see, for example, https://www.business.org/finance/cost-management/much-computer-cost/). For our cost analysis, $400 and $1500 seemed reasonable average cost bounds.

Since well-designed empirical studies on the type and frequency of firmware integrity errors contributing to PC replacement are unavailable (at least to this analyst), this note can only posit the potential cost savings. Confirmation of our premise is thus required in practice, so readers are encouraged to share their experiences. If PC replacement intervals are indeed extended and millions are saved, then firmware integrity tools will become immediately accretive.

About TAG Cyber

Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, Manhattan-based TAG Cyber bridges the gap between enterprise security practitioners and commercial cyber vendors. The company democratizes world-class research and advisory content and services, and provides a range of consultative solutions for businesses and government. TAG Cyber's security portal is used by organizations of all sizes to obtain timely, personalized security information.

DISTINGUISHED VENDORS

DISTINGUISHED VENDORS

2021

Since 2016, the TAG Cyber analysts have spent many, many thousands of hours carefully reviewing, sometimes enduring, but always providing honest advice to commercial cyber security vendors from around the world. This labor of love – and the crazy hours and low pay dictate that such insanely tough work cannot be anything but – creates deep insight into the industry for our team. In essence, we understand the security vendor space. (We do.)

From this day-to-day work, mostly by Katie Teitler, David Hechler, and Ed Amoroso, an impressive stream of articles results, usually covering some unique value proposition, belief system, or innovation noticed during a briefing. These articles are provided gratis in the hopes that the vendor of interest benefits from the attention, not to mention TAG Cyber's enterprise customers, who are nudged to have a peek at these select technology providers.

But, of course, this is no pay-for-play. The vast majority of time and effort spent each year by the TAG Cyber analysts involves no fees from vendors or enterprise buyers (a.k.a. our readers). So, we have the freedom to be honest – although we've made it our policy to substitute silence for nastiness. When we see a commercial solution that either does not compute or is being built for the wrong reasons, then we just silently cease to engage. We do not criticize.

In contrast, when a commercial vendor reviewed in our articles, which generally number about 250 per year, exhibits some belief, perspective, or approach that is deemed to be particularly interesting, then an arrangement is often negotiated whereby TAG Cyber and that vendor agree to cooperate for a year of joint work. They get a barrel-full of additional content, and we learn their area. Total fees hover around the price of a conference booth. We do not gouge.

Following are the commercial vendors who passed through our difficult gauntlet. If one recognizes that we actually track about 2,000 commercial vendors in our database, the ratio of that larger universe to the final tally below is about one in forty. We can thus confidently state that the companies listed below will bring enterprise buyers a nice experience. This is based on detailed and intimate interaction where we gain firsthand experience with the company.

TAG CYBER DISTINGUISHED VENDORS

2021

Whether you engage with these companies is something you can determine – or (warning: marketing message coming) you can give us a call at TAG Cyber. We do enjoy working with enterprise teams to optimize their security architecture, program, and vendor mix. We have a super unique, on-demand approach to this task – and we think you'll like it. So we do hope that you consider contacting us on our website.

One last minor point regarding our little acknowledgment write-ups below: The majority of vendors we deal with have asked that we reference the company rather than individual executives or employees we might have worked with during the year. This is a vibrant industry and people move often, so we respect that request. But for the wonderful people who have helped us during 2020 and into 2021, we offer our collective and heartfelt thanks.

ALLURE SECURITY

The challenge of combatting website spoofing has long suffered from few good options from commercial vendors, so we were so delighted to meet the team from Allure Security. Their unique approach to the problem helps enterprise teams reduce brand risk, while also addressing many if the issues that arise with phishing attacks.

Arctic Security

At TAG Cyber, we've come to see the value for enterprise teams in obtaining early information about breaches – and this led us to Arctic Security, a company that is pioneering the automated notification of cyber threat and vulnerability management data to customers. We are so appreciative of their support helping us develop insight into this approach.

AT&T

The team members at AT&T have been wonderful supporters of TAG Cyber since our inception. We genuinely appreciate the accurate insights and experienced guidance from AT&T on all matters related to mobility (especially 5G) and innovation in telecommunications. This helps direct our advisory work in network security.

Attivo NETWORKS

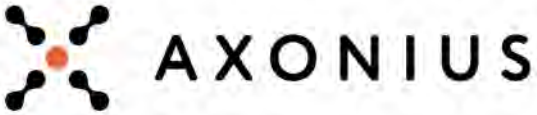
When it comes to deception, Attivo Networks knows its stuff. For several years, the team at Attivo has been so generous to invest many hours helping us understand this important aspect of cyber security. Their advice is especially appreciated because it comes from a deep understanding of the practical issues that arise supporting deception in enterprise.

TAG CYBER DISTINGUISHED VENDORS

2021

The idea to support authorization in a manner that provides more power and flexibility to end-users is one of the great innovations from Authoriti. We spent many hours going through the secure use-cases that emerge with their unique approach to frictionless transactions that reduce fraud, especially in financial services.

It is impossible to build a secure enterprise architecture without a network detection and response solution that can identify users, devices, and applications quickly – to detect anomalies before they can progress into attacks. Awake Security does this well, and they were so kind to spend time helping learn how this can be applied in practice to enterprise.



Sometimes the most important aspects of an enterprise security solution are the least flashy, so when we learned how the Axonius IT asset inventory platform and associated methodology worked, we were excited to dig deeper and to share with our enterprise clients. We are so grateful to Axonius for sharing their insights and experience with us.

Shifts toward securing APIs led the TAG Cyber team to spend countless hours with Cequence to learn in the ins and outs of this emerging area. Much of this learning resulted in an excellent, co-authored eBook on the topic, and our work with Cequence has helped us extend useful advice to many teams trying to better secure their APIs.

Continuous monitoring, enforcement, and control of cloud infrastructure for security is imperative in modern enterprise infrastructure. The team at CloudKnox has been so generous to share their understanding with our TAG Cyber team, and we've been able to better provide guidance in how properties such as least privilege can be extended to multi-cloud.

The CloudPassage team has been a world leader in the drive toward automated protection of virtualized workloads in public, private, and hybrid cloud environments. We are so appreciative of their continued support.

TAG CYBER DISTINGUISHED VENDORS

2021

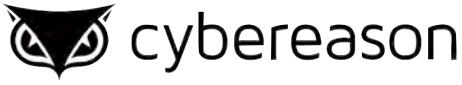
Security operations teams understand the value of training and simulated exercises and the team at Cloud Range has helped the TAG Cyber analyst team understand how this is best provisioned and performed in practice. We appreciate the insights and expertise of the Cloud Range team and our enterprise customers have benefitted from their kind assistance.

The insider threat to enterprise has risen from a minor issue a decade ago to possibly the number one concern amongst the chief information security officers we deal with at TAG Cyber. Code42 has been a wonderful partner to help us understand the best ways to mitigate this significant concern. We are grateful for their kind assistance.

Even with massive investments in secure email infrastructure, including secure email gateways, enterprise teams continue to see malicious phishing leaking through to in-boxes. Cofense helped us understand how crowdsourced human support can greatly enhance the end-to-end security for email and phishing. Their expertise has been valuable for our enterprise clients.

The ControlCase team spent considerable time with our TAG Cyber analysts to help us understand the specifics of how continuous compliance and security monitoring can be done for modern organizations. We learned so much from their experienced team and are now evangelists to continuous compliance for every business.

The concept of virtualizing front end network processing, as in a load balancer, is a creative means for implementing flexible security policies, and provides a new way to introduce virtual firewall capabilities to an enterprise. Ottawa-based Corsa has been a leader in this area of cyber security and we appreciate their time and effort helping us learn this valuable method.



Enterprise teams understand the importance of endpoint security in their overall protection architecture, and few teams have deeper insight than Cybereason. We are so appreciate of time invested by their experts to help us gain visibility into the key trends in endpoint technology, applications, and risk reduction.

TAG CYBER DISTINGUISHED VENDORS

2021

CYBRARY

Cybrary is one of the few companies that truly understands the specifics of how best to combine a professional learning experience with the nurturing guidance of a supportive community. We've enjoyed our involvement with the Cybrary team and have found our joint courses to be so satisfying. Thanks to the Cybrary team for their partnership and support.

Hackers tend to talk about their exploits, and the CYR3CON team has invented amazing technology that allows enterprise customers to gain insight into such discussions to enhance their threat intelligence. We've enjoyed our work with CYR3CON, including reading their technical books outlining the underlying foundational methods.

The team at Digital Defense has been a wonderful TAG Cyber partner for years, and we depend on them for insights into modern vulnerability management. They've been so kind to invest the time and effort to help us learn, and we truly appreciate their support of our program since we began. Our customers benefit from our interactions with this fine company.

Despite trends toward increased focus on application software, we all know that underlying threats to firmware and hardware remain a critically important concern. Eclypsium has been so kind to help the TAG Cyber analysts understand the best means for reducing risk in this area, and we've so enjoyed our joint work together.

Enabling secure collaboration, email, and related enterprise services is a critically important aspect of modern cyber security. We are appreciative that the Egress team has been so willing to invest time and effort to help our TAG Cyber analysts gain insight into the most effective methods to reduce risk and enhance productivity.

Securing identities in the cloud has been one of the more nagging issues in modern enterprise security. Ermetic helped us learn how this can become an important differentiator in a security program. We appreciate their time helping us better understand how cloud identity can include granular policies such as for least privilege. Thanks to the Ermetic team.

TAG CYBER DISTINGUISHED VENDORS

2021

The creation of synthetic data is an excellent way for vendors and enterprise teams to avoid the use of live, production data during any test or proof-of-concept activity. ExactData has implement excellent algorithms and technology to create such data and we've benefitted from their guidance on how this aspect of the security equation can work.

When a security team identifies its full set of risks, it often misses many of the more critical challenges that emerge on the Internet, outside they normal enterprise context. Expanse was kind to share their deep insights into this important area, and we learned much about how to create an accurate view of an organization's real attack surface.

The Fortinet team has been a leader in the integration of advanced cyber and network security solutions into a comprehensive fabric. We are so appreciative of all the fine support and assistance they provide for our analyst team. We learn so much about enterprise security from Fortinet each time we work together.

Truly iconic companies in cyber security are far-between, but HP stands out in its determination to provide a suite of products that not only support cyber security, but that actually play a key role in reducing risk to an organization. The TAG Cyber team is so grateful to HP for its kind support of our program and we appreciate the partnership.

The shift in virtually every aspect of modern computing from passwords toward a passwordless experience has been both supported and evangelized by the entire HYPR team. We continue to be impressed with their expertise, experience, and fine platform which helps enterprise teams reduce risk and cost in their employee's day-to-day authentication needs.

The Imperva team has done a great job curating what has now become an iconic brand in cyber security. They were kind to provide considerable guidance and information for the TAG Cyber analysts to learn how web application security is evolving. We are so appreciative of their assistance to help us pass our learning on to enterprise users.

TAG CYBER DISTINGUISHED VENDORS

2021

The team at InCyber has done a good job creating an alternate means for improving the accuracy and usefulness of user behavioral security. The TAG Cyber team has long believed in advanced behavioral analytics and we are appreciative of the discussions we had with InCyber on how this important technology is evolving.

Enterprise use of cryptography is one of the most critically important functions that can be easily overlooked by managers. The Keyfactor team offered amazing insights into enterprise key management, and we learned so much through our various technical interactions. Thanks to the Keyfactor group for their support of TAG Cyber.

It is hard to say anything about Microsoft that introduces much new the conversation – but we can report that this massive company treated the TAG Cyber analysts (admittedly a smaller team) with great respect. They helped us learn their strategy, and we developed deep insights into how Microsoft will enhance enterprise and cloud security in the coming years.

Securing email remains one of the most important aspects of modern enterprise security. Mimecast has been an industry leader in this key area for many years – and we are so appreciative of their support this past year helping the TAG Cyber analysts better understand the most successful methods for securing email and other means for collaboration.

One of the most iconic tools of all time in cyber security is the EnCase forensic toolkit, which digital forensic experts have been using for many years. OpenText, as the parent organization for EnCase, has done a wonderful job integrating the platform into its more general portfolio of enterprise software – and we appreciate their kind assistance helping us learn.

The PerimeterX team helped us gain deeper insight into the management of bot attacks, avoidance of client-side attacks, and mitigation of ad injection. Each of these defenses has the goal of enhancing the security and integrity of web and mobile applications. We are so appreciative of their support of our program.

TAG CYBER DISTINGUISHED VENDORS

2021

proofpoint.

Protecting enterprise from email threats has become perhaps the most important aspect of modern cyber defensive architectures – and Proofpoint is a clear leader in this area. We are appreciative of Proofpoint, and their recently acquired ObserveIT team, for helping us understand best practices in email security and user behavioral analytics.

Randori

The need for a continuous attack platform has gradually emerged as an essential component of any modern secure enterprise. The Randori team was kind to offer their insights and guidance to the TAG Cyber analysts so that we could share the benefits of an automated attack platform with our own enterprise clients. Thanks to the Randori team for their support.

REDSEAL

The TAG Cyber analysts enjoyed learning from RedSeal how world class enterprise security organizations use network maps as the basis for identifying potential risks, through deeper insight into how applications, systems, and networks are interacting. We are so appreciative of the time RedSeal spent helping us learn.

TAG CYBER DISTINGUISHED VENDORS

2021

RedShield

Web security has been examined from many different angles in the past decade, but the approach taken at RedShield – namely, to create shields around applications, struck the TAG Cyber team as particularly creative and important. We are so enjoying our interaction with this fine team from New Zealand.

respond

Security operations center (SOC) teams understand now that they will benefit from the use of a platform that supports autonomous decision-making. Respond Software is an industry leader in this important area – and the TAG Cyber analysts are so appreciative of their willingness to provide insights into how such automation can enhance SOC capability.

SailPoint

It's been such a pleasure to work with Sailpoint this year – and we are certain that as identity management and governance truly emerge as the primary means by which enterprise teams protect infrastructure, Sailpoint will continue to serve as a global leader. We appreciate their willingness to help us learn.

SecurityScorecard

The provision of a meaningful security risk score for an organization offers so many wonderful advantages for compliance, threat avoidance, risk reduction, and third-party management. The SecurityScorecard team was generous to help TAG Cyber learn how this capability is best deployed in the most capable enterprise environments.

SEMPERIS

Too many enterprise teams forget to adequately address the risks of Active Directory, and also every enterprise underestimates the consequences of availability issues with their directory services. Semperis offers a creative solution to the Active Directory availability risk with a unique platform the ensures rapid restoration in the case of a serious outage.

SentinelOne™

Endpoint security has emerged as a primary control in zero trust networks, and SentinelOne has emerged as a clear leader in this area. Providing excellent context for security teams is one of the advantages SentinelOne offers, and the TAG Cyber team spent considerable time digging into their fine technology, which continues to produce excellent results in practice.

TAG CYBER DISTINGUISHED VENDORS

2021

Rogue device proliferation on enterprise networks is one of the more underestimated and poorly understood aspects of cyber security – and few technology companies understand this risk better than Sepio. They helped the TAG Cyber team gain insights into the best ways to reduce this risk, including providing planned assistance to our partner students at NYU.

Protection of data is one of the most essential aspects of enterprise security, and the team at Sertainty has pioneered the idea of embedding intelligence into the data. This creative introduction of smart control into data has been one of the more interesting areas covered by our TAG Cyber analysts. Thanks to Sertainty for their continued support.

The concept of sharding data across disparate locations has been an increasingly popular way to achieve high levels of protection and robustness. ShardSecure offers a world-class means for taking advantage of this concept to protect data in multi-cloud infrastructure. Thanks to the ShardSecure team for helping us understand this important area of cyber security.

The WAF has always been an important component of the application security architecture, but Signal Sciences has pioneered the introduction of valuable next-generation WAF capabilities that are designed to integrate with DevOps, cloud, and virtual infrastructure. We so enjoyed our amazing learning from this world-class team at Signal Sciences.

Spirent has been a market leader for many years in the area of test, assurance, and automation for networks – and their suite of cyber security solutions is world-class, including their new continuous compliance solution. Thanks to the Spirent team for working so closely with us and supporting such an enjoyable and useful partnership with TAG Cyber.

Crowdsourced security testing has transitioned from a preferred option for enterprise to an absolutely mandatory control. Synack has been at the forefront of this evolution for many years, and the TAG Cyber analysts have enjoyed their willingness to invest time and effort to help us gain insights into the critically important area.

TAG CYBER DISTINGUISHED VENDORS

2021

Telos is a world-class corporation that supports enterprise and government with cloud, network, and security solutions that all support continuous assurance. The TAG Cyber team is so appreciative of their partnership this year, and it's been our pleasure to work with their fine experts to hep tell the Telos story of risk reduction and information assurance.

The use of a threat intelligence platform in enterprise has become a requirement for optimal cyber security protection. ThreatQuotient provides a world-class solution in this area, and they were so kind to invest the time and effort to help the TAG Cyber analysts understand how a threat-centric approach to operations can significantly improve posture.

The Trail of Bits team is truly unparalleled in their expertise and willingness to dive into the most complex cyber security problems. Our industry benefits not only from their fine work, but also from the world class tools they deliver to the cyber security community. We are appreciative of their partnership and support.

Deception is an area that our TAG Cyber team has long considered to be critical to the reduction of risk in the enterprise. We so enjoyed working closely with the TrapX team to understand their approach to simplifying the deployment and use of deception in business. We appreciate their willingness to invest time to help us learn.

The Truefort team has been one of our go-to partners when we need to understand the nuances of application security, especially in the context of non-trivial enterprise software. We've been so impressed as the company has matured into one of the world's leaders in protecting business critical applications from attack.

The TrustMAPP team drives a new discipline called security performance management that we embraced fully at TAG Cyber in our program this past year. With the goal of offering continuous, automated assessment of posture, TrustMAPP provides an essential component of the modern enterprise security program. We are appreciative of their assistance and support.

TAG CYBER DISTINGUISHED VENDORS

2021

vArmour

The TAG Cyber team has long admired the work of vArmour in advancing the cause of cloud-hosted application security. More recently, their introduction of application relationship management is a concept we have embraced and shared with our own enterprise customers. Thanks to vArmour for their continued industry leadership.

WALLIX
TRACE, AUDIT & TRUST

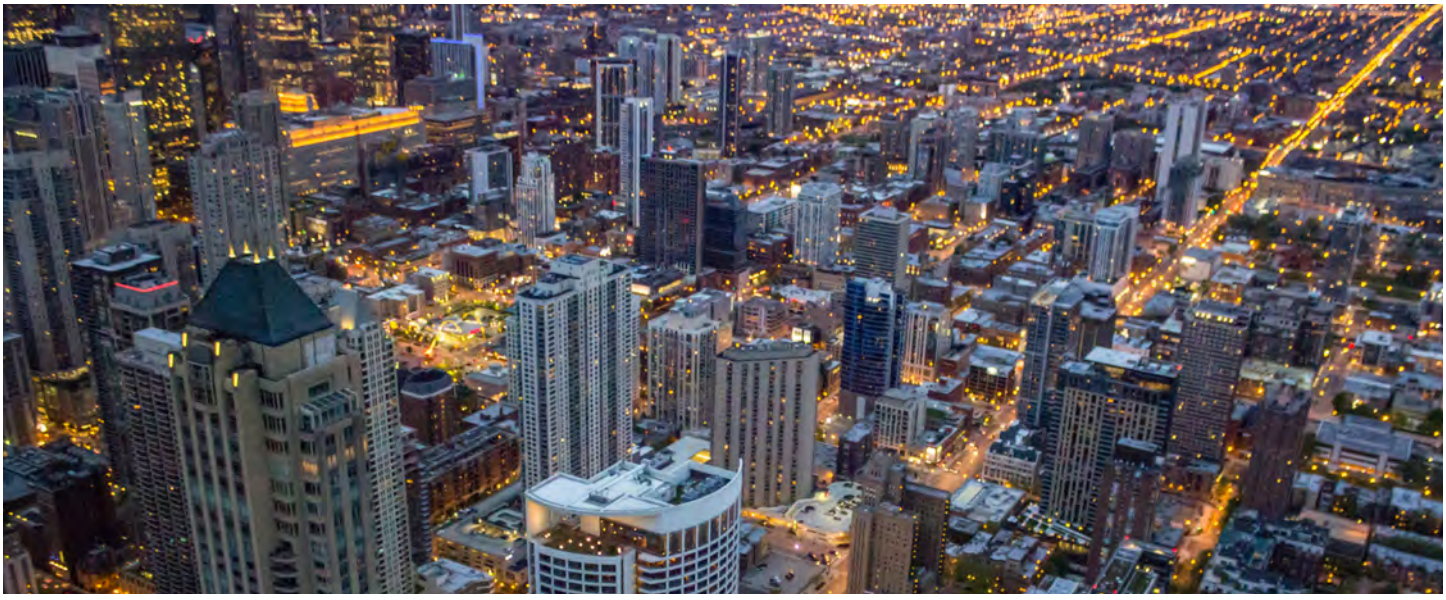
France-based Wallix was such an amazing partner this past year helping our TAG Cyber team learn the specifics of how modern privileged access management (and related controls) are best applied in the enterprise. Their solution suite has evolved to world-class and we are appreciative of their kind support of our program.

WATERFALL®
Stronger Than Firewalls

The Waterfall Security team has been a wonderful partner in the area of industrial control security – and, in particular, in the provision of unidirectional gateways for advanced protection of operational technology infrastructure. The TAG Cyber analyst team is grateful for their kind investment of time and effort helping us learn.

XBAND

We have been enjoying our work with Xband this year as they reinvent the notion of providing an advanced cyber security solution for enterprise. We've watched the evolution of both managed security and valued added solutions in our industry. Xband understands both and is well-positioned to create a differentiated offer.



TAGCYBER