

TAG Cyber •
Security Annual
2ND QUARTER 2021

**MARKET OUTLOOK &
INDUSTRY INSIGHTS**

WELCOME TO THE 2021 TAG CYBER SECURITY ANNUAL – 2ND QUARTER EDITION

We are pleased to offer our peers, customers, colleagues, and friends in the cyber security community this volume of original articles, analyst reports, and yes – more original cartoons. The goal of our Quarterly is to inform, challenge, and entertain our readers. We hope you find the cyber security material helpful in your day-to-day work as practitioners, managers, vendors, educators, researchers, government officials, and investors.

While it's only been a few months since the publication of our first **Quarterly**, we see many changes in the cyber security community and even more broadly in the business world. While Q2 2020 ushered in some dramatic changes in business operations and working environments, Q2 2021 is continuing many of those changes while introducing yet another challenge: hybrid working environments.

Why is this such a big deal for cyber security?

In the rush to accommodate a mass exodus from the office to work-from-home, security teams made concessions—at first—to grant access to home and remote workers, allowing them to do their jobs as well and as easily as possible. Baselines were then established (albeit ones that were abnormal) to understand new work-from-home habits, devices, and access needs. For nearly a year, the abnormal became the norm.

And during this time, executives saw that this flexible work environment was good for many more people than expected. It benefitted workers and businesses, alike. Now, then, as we see the light at the end of the pandemic tunnel, businesses are strategizing on their new operating plans, looking to incorporate more flexible options for a greater percentage of their workforce.

But the constant, continuous change precipitated by the allowance of both work-from-home and remote work introduces new security challenges. The mixed use of personal and work devices for work purposes, unmanaged devices touching corporate resources, perpetually shifting user locations and thus use of various connectivity options, and more all lead to the need for fine-grained control of access rights, highly-tuned behavioral monitoring, hardened data and application protection, increased device hygiene, improved cloud configuration management, and on and on the list goes.

Cyber security has never been for the faint of heart, nor the complacent. But in 2021, we have to work through myriad, fast-moving challenges at once, without dropping the ball on security while supporting a hybrid work environment that allows employees, contractors, and partners to work seamlessly, wherever and however they need or want to work.

And of course cyber attackers know that security defenders' attentions and resources are spread thin. The SolarWinds attack and its ongoing, far-reaching repercussions continue as we write this second quarter Quarterly. Microsoft experienced a severe attack against its Exchange server, impacting thousands of customers. Molson Coors was shut down temporarily after a cyber attack. Buffalo, New York public schools suffered the same fate. A water treatment plant in Florida was compromised due to a remote access vulnerability and the attacker was able to temporarily (and fortunately minimally) adjust the amount of lye added to the water. IBM Security reports a near-50% increase in attacks against vulnerabilities in industrial control systems over the past year. And more concerning attacks and incidents will occur between this writing and its publication in a month.

Continued

INTRODUCTION

Continued

Enterprise security teams understand the scope of the problem and are now working on strategies and adopting technologies that can handle modern threats. Zero trust principles and data- and application-centric approaches are being adopted at the world's leading organizations, and vendors are rising to the challenges. But the road is long and there's much work still to do.

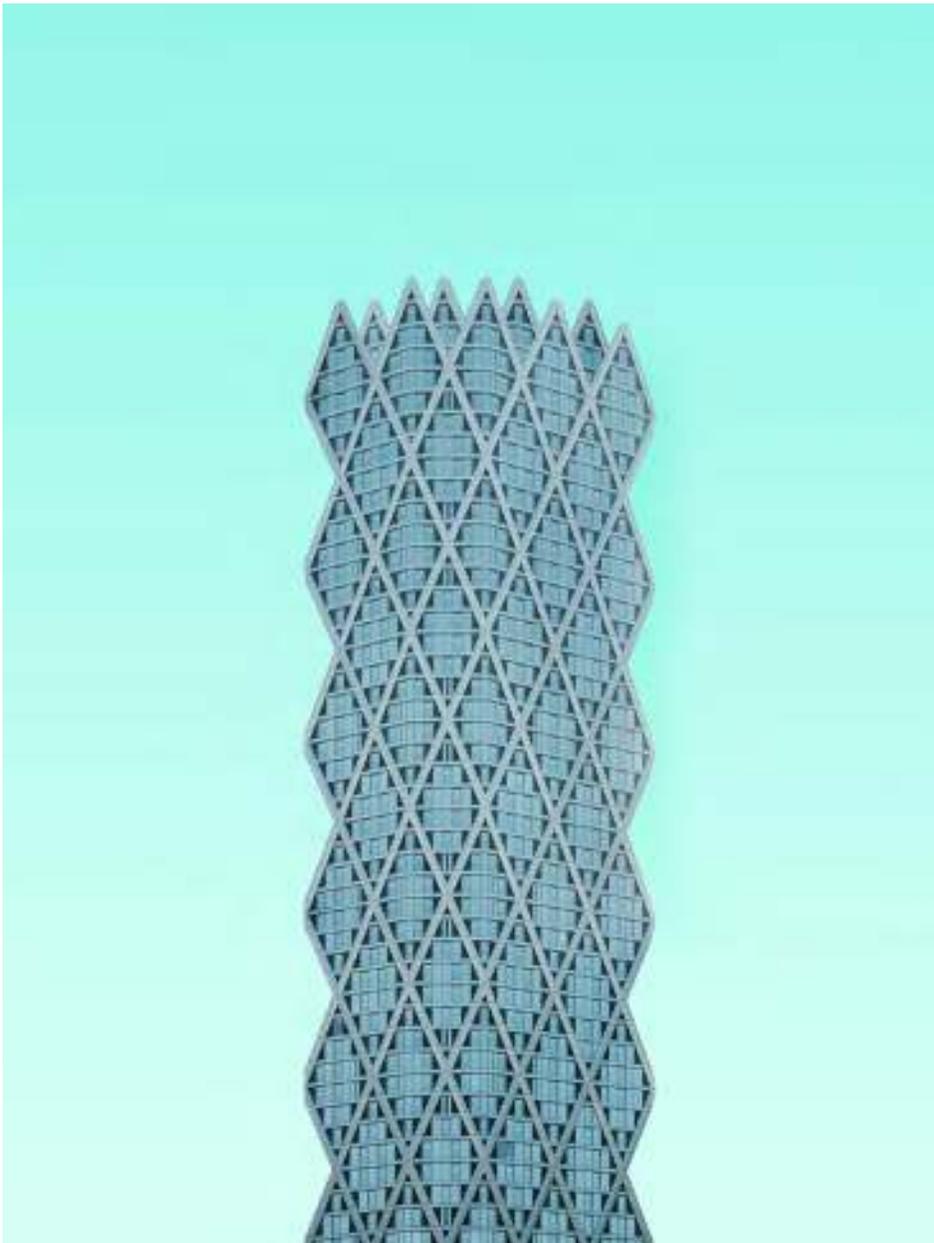
We at TAG Cyber are working furiously with enterprises and vendors to connect needs and capabilities, and we know we're only a fraction of the puzzle. We're expanding our research services via a new research subscription that provides deeper insights and more detailed information, especially on commercial vendors—large and small, paying customers and not—for enterprises, and we're building a portfolio management tool for enterprise to better streamline their investments in security technology.

In this Q2 2021 Quarterly, you'll see TAG Cyber's continued commitment to frank, honest, and unbiased research about our industry. We hope you find some inspiration in the articles and reports, and we promise to continue pushing ourselves to provide guidance that is practical and useful.

We also encourage you to reach out; we wouldn't fulfill our promise of democratizing cyber security research if we weren't open to conversations with enterprises and vendors, regardless of their contractual status. We know you, the practitioners, have great insights that we don't always experience firsthand anymore, and we welcome your thoughts and ideas.

For now, enjoy the second edition of the TAG Cyber Quarterly. Read, learn, and laugh (at our cartoons), then go forth and secure!





FEATURED PHOTOGRAPER
Simone Hutsch / Unsplash

- **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** – Lester Goodman, Miles McDonald, Rich Powell

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871
Copyright © 2021 TAG Cyber LLC. All rights reserved.

This publication may be freely reproduced, freely quoted, freely distributed, or freely transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system without need to request permission from the publisher, so long as the content is neither changed nor attributed to a different source.

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the authors of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2021 TAG Cyber Security Annual volumes.

The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.

The opinions expressed in this document are that of the TAG Cyber Analysts, and in no way reflect that of its Distinguished Vendors.

January 22, 2021

C O N T E N T S

Introduction	2	Prevent Bad Code Commits from Causing a Megabreach Om Moolchandani, Accurics	52
Overview of the TAG Cyber Controls for 2021	6	How to Gain Control of the Hardware Supply Chain Yossi Appleboum, Sepio Systems	55
OP-ED	8	Amp Up your Security Program with your Security Consulting Partner Tim Wainwright, SRA	58
The Time Has Arrived for Software Bill of Materials	9	Data Authorization with Privacy by Design Nong Li, Okera	61
Critical Infrastructure Attack Reveals Why Access Should be The Nexus of Your Security Program	14	Using Passwordless Authentication to Eliminate Attack Vectors and Provide Secure Access Ori Eisen, Trusona	64
From Third-Party Risks to Third-Party Partners	16	Eliminate Easy Targets in your Firmware John Loucaides, Eclipsium	67
Is Ransomware Here to Stay? 3 Trends to Expect in 2021	18	Using Emulation to Fight Against Gravity with Limited Resources Bryson Bort, SCYTHE	70
5 Steps to Turn your MSP into an MSSP	21	Contextualizing Data Protection with SASE Jason Clark, Netskope	73
7 Tips for Giving Meaningful Demos	24	ANALYST REPORTS	76
Note to Cyber Startups: The First \$3M is the Hardest	27	Protecting Digital Identity from Cyber Compromise	77
The Growing Obsolescence of Credentials	29	Maximizing Open Source Security Tools by Engaging and Open-core Vendor	84
A New Program Assesses Law Firm Security	33	Packet Capture is a Foundational Technology	89
Want to Stop Nation-State Cyber Threats? Simplify.	35	How Enterprise Security Teams Benefit from Cloud Infrastructure Entitlements Management (CIEM)	95
INTERVIEWS	36	Account Takeover Protection: How to Stop ATO	100
Data Governance and Data Privacy: Sources of Business Growth Monica Dubeau & Cynthia Luu, IBM	37	DISTINGUISHED VENDORS	107
A Holistic Approach to Infrastructure, Data, and Device Cyber Protection Candid Wuest, Acronis	40		
Are you Blind and Exposed to Too Much Cyber Risk? Gaurav Banga, Balbix	43		
Is your Email what It Purports to Be? Roger Kay, INKY	46		
How Secure is your Microsoft SaaS Deployment? Do you Know? Aaron Turner, Sirix	49		

OVERVIEW OF THE TAG CYBER CONTROLS FOR 2021

Each year, our expert industry analysts review and update a list of what we refer to as the TAG Cyber Controls. Our list is best interpreted as those areas in which a Chief Information Security Officer (CISO) must include focus in their enterprise security program. The TAG Cyber Controls represent our best answer to the following question that we hear almost every day from CISOs and their teams: *What elements should I include specifically in my enterprise security program?*

We understand that many might choose to answer this question in terms of existing security frameworks. For example, we have the comprehensive NIST Cybersecurity Framework (CSF) and its detailed security requirements in NIST 800-53 (rev 5). We also have the smaller and more accessible Center for Internet Security (CIS) Controls, which boils things down to twenty functional recommendations to reduce enterprise security risk.

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

Continued

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

Our belief at TAG Cyber, however, is that none of these frameworks are sufficient for our industry research and analysis, and none match our collective experience running security programs, managing enterprise protection, and coaching CISOs across every sector. Instead, the frameworks always include something important *just slightly off* in their coverage. What industry CISOs, for example, actually use the many pages of documentation in NIST as a practical guide?

THE CONTROLS

We developed the TAG Cyber controls based on practical experience. The framework includes familiar areas such as firewall platforms and multi-factor authentication, but it also includes newer strategies such as deception platforms and managed detection and response (MDR) vendors. Furthermore, the framework provides our subscription customers direct linkage to categorized lists of commercial vendors, rather than pages of detailed sub-requirements.

The TAG Cyber Controls are presented to support visual inspection at a glance, which explains why many refer to it as the Periodic Table of Security. CISO-led teams now use the fifty-four controls as a checklist to determine the completeness and accuracy of their program. Consultants can also use the framework to help clients assess the appropriateness of their security program without having to deal with the academic and often impractical requirements in other compliance criteria.

Readers of previous versions of this TAG Cyber report should note that some changes have been made to the framework for 2021. We expect this to continue as we monitor the industry, review new trends, and work with CISO-led teams. The changes are subtle, but important – because they help to ensure that our control structure is complete and accurate. We work hard to ensure no gaps in our treatment, so that your program can avoid exploitable seams.

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 various entries. Admittedly, the categorization is not perfect, and any security 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.

To review our control details visit: www.tag-cyber.com/advisory/controls



OP-ED

THE TIME HAS ARRIVED FOR SOFTWARE BILL OF MATERIALS

EDWARD AMOROSO

The benefits of Software Bill of Materials (SBOM) are outlined in the context of standards such as SWID and SPDX from NTIA, ISO, CycloneDX, and the Linux Foundation. To address challenges in implementation, a maturity model is proposed here to enable use of SBOM in practical software procurement settings.

INTRODUCTION

Allan Friedman from the US Department of Commerce illustrates a bill of materials this way: “Twinkie buyers often assume the product to be vegan,” he says, “but a glance at the list of ingredients reveals use of beef fat.” Yecch. Now – after the inevitable joke that even hungry rats sniff-and-pass at Twinkies, one must admit that if junk food makers can be forced to share their ingredients, then so should software providers.

Stated simply – the time has arrived for a software bill of materials to accompany any code being delivered into a consequential setting, which means pretty much all software. Blessed with a pronounceable acronym – SBOM, the concept seems to polarize observers into two camps: The true believing camp and the no-way-you-can-do-it camp. Below, we examine both arguments – and hopefully convince you that the title of this article is correct.

Specifically, we cover the major arguments for and against SBOM, including a summary of ongoing contributions from several major organizations including NTIA, ISO, CycloneDX, and the Linux Foundation. We also propose here an SBOM maturity scale that allows software providers to provide guidance on the level of assurance that exists in their SBOM. Such claims should assist buyers in their software procurement activity.

CASE FOR SBOM

The conceptual notion of a software bill of materials is simple: Buyers of software would demand a nested inventory of the components used to develop the product or system. The resulting transparency would help buyers establish higher levels of assurance for software

The approach has the potential to help address the crisis the security community is currently experiencing in supply chain risk management.



developed from components deemed desirable – and of course, lower levels of assurance for software developed from components deemed undesirable.

The approach has the potential to help address the crisis the security community is currently experiencing in supply chain risk management. That is, by better understanding the underlying composition of software used by downstream suppliers and partners, an organization can develop a comprehensive view of its dependencies and hopefully respond more quickly to security vulnerabilities in both well-known and obscure software components.

The National Telecommunications and Information Administration (NTIA) within the US Department of Commerce has been a leading proponent of this concept in industry. They have developed a rich set of online resources that explain in detail the many benefits of SBOM use, including transparency goals, supply chain advances, and discovery options. NTIA makes a compelling case for SBOM – and enterprise teams would be wise to become more educated.

Similarly, the CycloneDX community has created an object model consistent with the OWASP Dependency Track, which supports the development of many open source and proprietary SBOM tools. Like most open source projects under the Apache license model, CycloneDX has benefitted since its inception in 2017 from the SBOM-related technical contributions by its global community members.

SBOM-RELATED STANDARDS

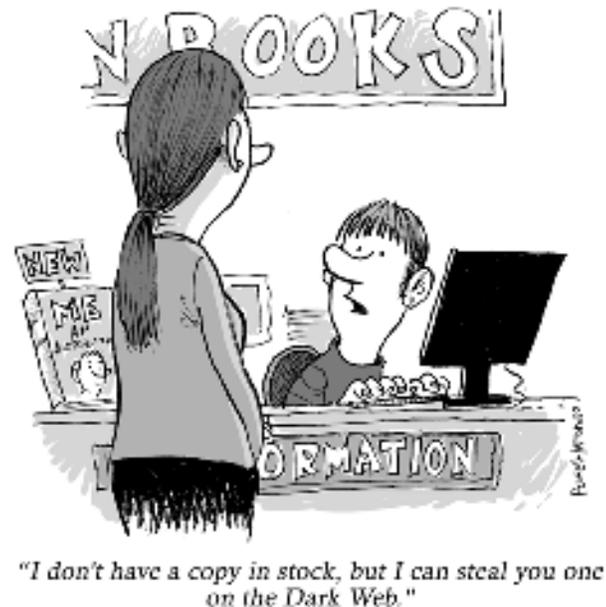
Perhaps the most impressive aspect of this push to SBOM involves the establishment of standards for how such software ingredients would be listed and used. Obviously, for an SBOM to be useful, buyers must understand what each component means – or to have a process for establishing such understanding. (In the Twinkie case, for example, the actual beef fat ingredient is listed as tallow – which might require a quick Wikipedia search to identify.)

Several standards have been established for SBOM. One is called Software Identification (SWID), which is an ISO/IEC 19770 format used by many commercial software vendors today. Another commonly cited standard is called Software Package Data eXchange (SPDX), which is an open-source machine-readable format driven by the Linux Foundation. The standards are complementary and typically used in different parts of the software lifecycle.

SWID tags provide a standard means for defining metadata about a software product. Managed by ISO and IEC, SWID tags define product versions, organizations involved in product development, information about artifacts used to create the product, and relationships between the product and other software. The common goal for both SPDX and SWID is to improve the underlying metadata through commonly used standards.

SPDX specifically documents information on the software licenses which apply to a given piece of software being distributed. It is managed by the SPDX Working Group, which is governed by the Linux Foundation. The goal is to standardize a meaningful set of metadata around

the components included in a bill of materials. If users cannot interpret this metadata easily, then an SBOM will not be effective.



The types of data included in SPDX can obviously evolve, but current use includes the following main types of information:

- Document Creation: Defining the SPDX document creation process supports forward and backward compatibility for processing tools.
- Package Information: A package is a software product, container, component, or other logical grouping of items in a common context.
- File Information: The file information in an SPDX document includes metadata such as name, checksum licenses, and copyright.
- Snippet Information: Snippets define how content is included from other original sources. They denote when part of a file may have been created under another license.
- Licensing Information: The SPDX license list might not be comprehensive, so this section provides other license data that might be present in the software.
- Relationships: This includes definition of the relationships that exist between SPDX documents, packages, and files.
- Annotations: Annotations allow reviewers of an SPDX document and to pass on information from their review.

SBOM Lifecycle Model One effective lifecycle model for SBOM has been carefully designed by NTIA in the context of the typical ongoing software process. The idea is that SBOM actions should be directly integrated into each software process activity to help drive increased transparency and assurance for direct and downstream users of the software. A flattened representation of the continuous model is sketched below in Figure 1.

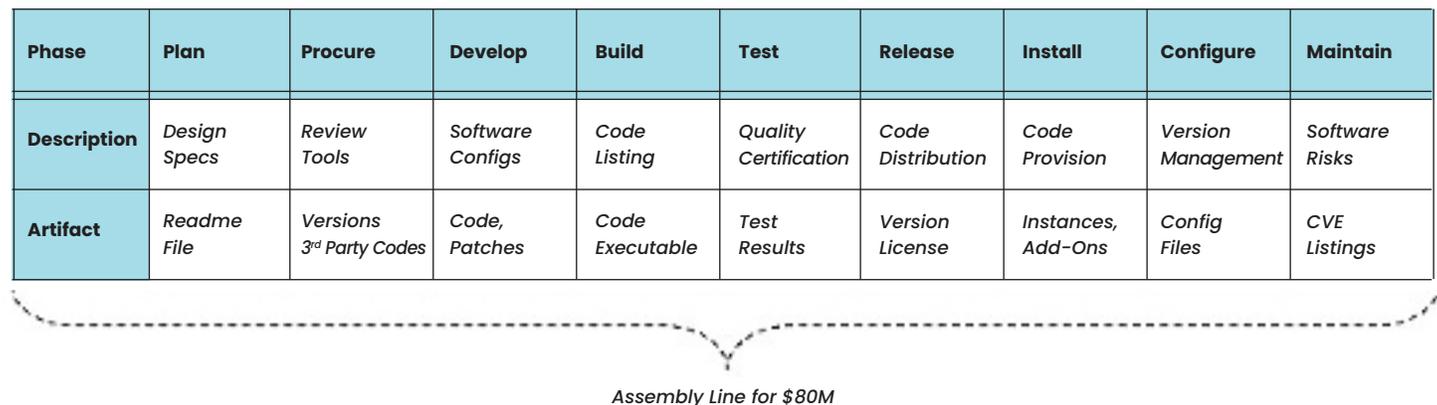


Figure 1. SBOM Lifecycle Model

The primary goal associated with practical implementation of an SBOM is that the tools and processes associated with the software lifecycle can be configured to automatically derive and accurately define the information that is stored in the SBOM. This can include code scanning

tools, source code management systems, version control platforms, compilers and build tools, security test platforms, package repositories, and app stores.

CASE AGAINST SBOM

Software experts have raised some reasonable questions about the feasibility of an SBOM. The first objection that SBOMs will not work centers on the level of accuracy and completeness of the data. Obviously, one cannot depend on an SBOM if users suspect that information about the materials and components added, removed, or modified during the software lifecycle is incomplete. Without full automation, this data is likely to be highly suspect.

This argument seems valid when one considers that while the number of possible commercial software licenses might be manageably small enough to track, the number of software components available in the open source community is enormous – and maintaining software version information complicates an already massively complex task. This concern will have to be addressed before SBOM can be applied at scale.

An additional objection is that stakeholders have no easy way to determine the security history

of some software component. If, for example, a software package has had vulnerabilities at some point in its existence and use, then there is no current means to accurately track this information. The data might have existed in a previous SBOM, but the standard does not define how this legacy information can be carried forward.

This challenge is troublesome because tracking software vulnerabilities has always been a difficult task. This implies that unknown vulnerabilities will not be captured in an SBOM, which would seem to undermine their use. Resources like the National Vulnerability Database (NVD) have been put in place to address the problem, but progress has been slow, and identification of software vulnerabilities remains an inexact process.

Ultimately, if a software provider hates the idea of an SBOM, then they simply will not develop one. If, on the other hand, they find that this cause challenges in the buyer marketplace, then presumably they would change this decision. The maturity scale we propose below is intended specifically to help with that decision by allowing software developers and buyers to ease into the process slowly.

AN SBOM MATURITY SCALE

To address the challenges of practical SBOM implementation, we propose here that buyers have access to a meaningful maturity model based on a scale of claims made by software providers. The scale we propose would initially have three levels corresponding to no SBOM, a partially implemented SBOM, and a high-confidence SBOM. Obviously, this scale graduates upward in effective guidance for software buyers.

The maturity model is based on three simple designations: First, a software provider would make the claim that they either do not use SBOM, have a partially developed one, or have a fully developed SBOM. Presumably, any software provider making no claim would be

OBVIOUSLY, ONE CANNOT DEPEND ON AN SBOM IF USERS SUSPECT THAT INFORMATION ABOUT THE MATERIALS AND COMPONENTS ADDED, REMOVED, OR MODIFIED DURING THE SOFTWARE LIFECYCLE IS INCOMPLETE.



designated at Level 1. Buyers would have to determine how much confidence to place in a given provider’s claim of maturity – but the factors are simple enough for this to be a relatively easy process.

Second, a software provider would offer justification for their maturity claim by offering guidance on the degree to which generation of an SBOM is done manually or using automated tools. Hybrid processes would presumably include both type of activity. It should come as no surprise that the maturity goal would involve full automation of SBOM, but providers should be reasonably permitted to support a hybrid approach if that results in a more accurate SBOM.

Finally, the confidence level associated with an SBOM could be an aggregate designation made by both software providers and also buyers. For Level 1, such designation is simple, but at the two higher levels, it is possible that providers and buyers might come to different conclusions based on available evidence. It is possible that a third-party maturity assessment might be meaningful, but this seems overkill given the simplicity of the model.

SBOM Maturity	SBOM Usage	SBOM Generation	SBOM Confidence
Level 3	Full	Hybrid/Automated	Moderate/High
Level 2	Partial	Manual/Hybrid	Low/Moderate
Level 1	None	None	None

Figure 2. Proposed SBOM Maturity Scale

ACTION PLAN

The SBOM community continues to drive the adoption of SPDX, SWID, and SBOM – and this activity should be encouraged. It may be premature for governments to mandate their use, but buyers can certainly begin to introduce the concepts to their procurement processes. This can be done by simply asking providers if they are working on an SBOM for present or future software. The maturity scale introduced here might assist in this regard.

CRITICAL INFRASTRUCTURE ATTACK REVEALS WHY ACCESS SHOULD BE THE NEXUS OF YOUR SECURITY PROGRAM

KATIE TEITLER

This article was published in February 2021 after it was broadly reported that a water treatment plant in Florida was the victim of a cyber attack.

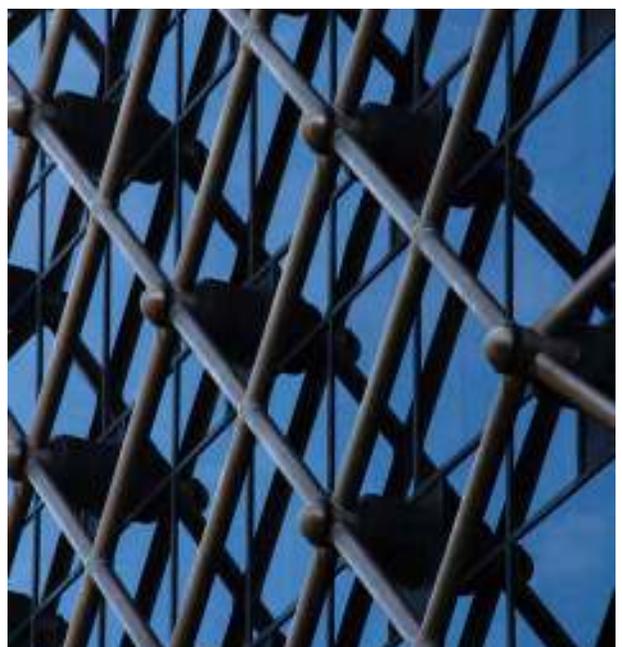
A cyber attack against a Tampa, FL water treatment plant is the latest reminder that security control of critical infrastructure must continually improve.

According to a report by Reuters, a cyber criminal gained unauthorized access to an employee's TeamViewer application (remote access and desktop support software)ⁱ and then used the access to gain control of systems that administer chemicals to the water supply. Per the nature of TeamViewer, the employee could see this happening in real time (fortunately he was on his computer at the time of the breach) and alerted supervisors who were then able to reverse the command and limit damage. No further details of the attack were provided in the report.

Quick action on the part of the employee and his supervisors ensured that the water treatment plant wasn't additionally tampered with. And official statements from the facility assure the public that supplemental controls are in place to prevent future damage of this sort. What if, though, this had been a savvier attacker who knew how to circumvent those controls? This is not some far-fetched SciFi fantasy. This is the reality critical infrastructure (CI) companies must face.

The number of connected devices and systems in CI is increasing all the time, thereby increasing digital risk. This is no different than any other company's attack surface. The bigger risk with CI, though, is the digitization of traditional industrial control system (ICS) and SCADA networks, systems not historically connected to typical IT networks. Nonetheless, despite the fact that operational technology (OT) cannot or cannot easily be managed,

TO PREVENT COMPROMISE, ORGANIZATIONS MUST LAY THE FOUNDATION OF CYBER SECURITY BY STARTING WITH IDENTIFYING, TESTING, AND IMPROVING ACCESS CONTROLS, AUTHORIZATIONS, AND PERMISSIONS.



measured, or monitored with traditional IT and security tooling, the IT/OT convergence has already occurred. This presents both risk and opportunity.

Despite any challenges, CI security and operations teams must implement technology and processes that account for the merging and interdependencies of IT and OT systems. They must realize that the exploit of an insecure software deployment can lead to great damage, like excessive lye in the water supply. All the typical cyber threat tactics facing private enterprises and government are also targeting CI—malware/ransomware, escalation of privileges, social engineering, botnets, denial of service. The risks of a missed control are higher, however, when human life is involved—that is to say, when a water supply facility, hospital, transportation authority, or like entity is the target of attack.

TRIED AND TRUE PROCESSES

Though stakes change, the process for protecting CI is similar for every organization. Every attack starts by exploiting the easiest vulnerability—the lowest common denominator—whether that’s insecure software, gaps in controls, or human error. To prevent compromise, organizations must lay the foundation of cyber security by starting with identifying, testing, and improving access controls, authorizations, and permissions. A compromised device, as was the case with the Florida water treatment plant, should not result in an attacker’s ability to affect chemical levels via manipulation of OT.

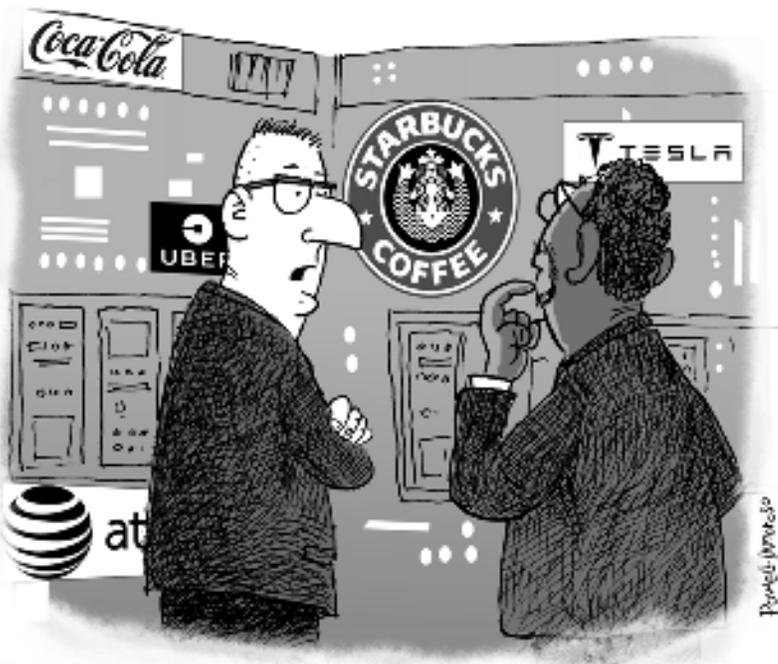
Access to a device should not offer carte blanche access to every system, program, or connected piece of software or hardware. Contextual and conditional access should be the rule, especially for high-risk systems. Behavioral monitoring, too, will mitigate risk when an attacker asks a system to do something outside the baseline or beyond restrictions. These steps are all part of a zero trust architecture based on workflows and functions.

Organizations need strategies, tactics, and tools that proactively prevent unauthorized access to resources. Access is the nexus of cyber security control. It is, for certain, not the only layer of security that must be applied, but it’s the best place to start. Realizing that determined attackers will find their way

into organizations’ networks regardless of endpoint controls, regulating access and the ability to interact with resources—whether that’s human to machine or machine to machine access—are crucial elements of the cyber security plan.

Systems properly protected with a zero trust framework that covers access controls, authorizations, permissions, behavioral monitoring, and, maybe most importantly context, are the key to preventing compromises like one TeamViewer wrought. It’s a simple concept, though one we know is often difficult to deploy. But that doesn’t mean you shouldn’t start somewhere. Why not access?

¹ This is far from the first time TeamViewer has been used in an [exploit](#)



*"We had to deal with the budget cuts **somehow.**"*

FROM THIRD-PARTY RISKS TO THIRD-PARTY PARTNERS

DAVID HECHLER

Bert Kaminski is an in-house lawyer who spends a good deal of his time as a director at Google Cloud. Previously he worked for a trio of tech companies, including 16 years at Oracle. So he's learned a few things about acquiring technology. And he had some interesting things to say.

There's a "misconception," he said, "that a company that is buying technology can impose all of its perceived security requirements on the seller." In other words, you can buy it and ask the seller of a standard product to re-engineer it to meet your specialized needs. "But if you have to do that," Kaminski said, "you're buying the wrong product."

His analysis applied equally to purchasing software or migrating to the cloud, he said. "You have to be happy with the products as they are. If you have to bring a vendor or service provider kicking and screaming to agree to all these one-offs, you are actually increasing your risk profile. It's probably introducing more complexity into your IT environment, which can present operational risks and new attack vectors."

We spoke for nearly an hour as Kaminski prepared for a discussion on mitigating third-party risk. He was one of four panelist on a University of San Diego webinar that aired on January 28. Our conversation jumped from vetting software to training employees to scoping out the suppliers of your suppliers. All of it touched on some form of risk. It was leavened by Kaminski's down-to-earth observations and practical advice. .

For example, we discussed the various ways employees can—intentionally or not—create cybersecurity risks. This is an area where in-house lawyers can play an important role, he said. They have expertise in data protection, privacy, and confidentiality. They can help provide training that reflects "the latest thinking of what regulators are looking for," he noted.

Then he added a word of caution. "I will say that lawyers should not be the only ones providing the training.

WHAT IF THE WEAK LINK IS NOT THE VENDOR YOUR COMPANY HAS A RELATIONSHIP WITH, BUT ONE THAT YOUR SUPPLIER DOES?



Because if they speak legalese, business people will tune them out.” Why? “They’ll think the training is just a make-work, check-the-box exercise,” he said. “So you want to be sure you’ve got business buy-in and sponsorship.” The employees need to know “that their management is part of this.” Lawyers can assist by lending authority, but the training will be more effective if it comes from the business—like someone from HR.

We turned to supply chain risk, which can be tricky. Especially the part that always struck me as a house of mirrors. Companies can be responsible for (read: liable for) breaches that occur due to the vulnerabilities of their vendors. What if the weak link is not the vendor your company has a relationship with, but one that your supplier does? In other words, the vendor of your vendor. Are companies supposed to conduct due diligence on all of their vendors, and then all of their vendors’ vendors?

It’s impossible to examine them all, Kaminski acknowledged. The best that a company can generally do is work closely with their direct suppliers and “hold them accountable.” But in some instances, he noted, it may be appropriate and even legally required for your suppliers to provide more detail. The EU’s General Data Protection Regulation, for example, requires any third parties you hire that process your data to inform you of any subprocessors involved. Beyond that, a company can insist that its suppliers describe and attest to their own security, and their due diligence in choosing and vetting their vendors. And a company can include terms in their supplier agreements that address breaches and other liabilities. But there’s no practical way to get a lot more granular than that, he said.

The big subject I wanted to ask about was not [SolarWinds](#), which we talked about briefly. It was how companies migrate to the cloud. How they vet and choose a vendor. How they work through the transition. How they manage security afterwards.

Before selecting a cloud provider, Kaminski recommended asking for lots of documents. To be sure you’re looking at a reputable provider, you want to see third-party attestations of security. If your own company works in health care, does the cloud service align with best practices in the field—the [HIPAA Security Rule](#) and the [HITECH Act](#)? “There are third-party reports and attestations for all of this,” he said. “And then you can send them supplemental questions.” Ask about their vulnerability testing, background checks on employees, encryption policies and procedures.

The big picture was that migrating to the cloud is not like going to Best Buy and picking out software, or even a larger purchase like a computer. It’s not a matter of paying, taking it home, and you’re done. “It’s not static,” he said. “It’s evolving.” The threat landscape evolves. The company’s needs evolve. All of a sudden everyone is working from home. You may need to have your system reconfigured to reflect these changes.

“This is not the old days, where somebody sends you a stack of [CD-ROMs](#), and you’ve licensed the software, and the relationship is pretty much arm’s length or over,” Kaminski continued. “Cloud isn’t just a transaction,” he emphasized. Cloud “is a collaborative, long-term relationship. And it’s one that expands.”

After so much talk about third-party risks, it was a pleasure to linger on third-party partners.

IS RANSOMWARE HERE TO STAY?

3 TRENDS TO EXPECT IN 2021

HAIDEE LECLAIR, GUEST AUTHOR

Now that the pandemic has shifted so many organizations to embrace a distributed workforce, cyber criminals are evolving to deploy new ways to take advantage of the abrupt shift. Nearly a year ago, as organizations in all industries scrambled to move their employees home, employees became more susceptible to some of the attacks that businesses were previously able to shield them from. For example, home internet connections are typically far less protected than corporate networks, and many organizations don't have a plan for managing the information on their employees' personal computers.

NEW ATTACK SURFACES WITH REMOTE WORK

With a wider attack surface and a workforce not accustomed to handling their own cyber security, ransomware attackers are alert to new opportunities. To increase the likelihood of payment, they are strategically choosing which target to strike – and when. A moment that's different in each industry, such as education and healthcare:

- Successful ransomware attacks on the education sector **increased 388%** in the third quarter of 2020, timing the attack with the return to school. This increased pressure on school districts to pay the ransom quickly rather than further disrupt a fractured distance learning deployment driven by the pandemic.
- With skyrocketing COVID-19 hospital admissions in late 2020, attacks on **healthcare** increased as cyber attackers bet on healthcare executives paying quickly to restore access. Researchers observed that the healthcare industry experienced more ransomware attacks since November 2020, **rising 45%**, more than double observed in any other industry.

Universal Health Services Inc. said a malware attack in late September cost the hospital chain \$67 million last year before taxes. Revenue dropped as patients went elsewhere for care, Universal Health said, and it incurred expenses to restore its operating systems. – Wall Street Journal

CYBER ATTACKERS MADE AT LEAST \$350 MILLION IN 2020, ACCORDING TO CHAINANALYSIS, SO THEY AREN'T GOING TO STOP RANSOMWARE ATTACKS IN 2021.



WHAT TO EXPECT FROM RANSOMWARE ATTACKS IN 2021

- **Double extortion attacks.** Criminals paralyze systems *and* threaten to release personal or sensitive data. This adds considerable urgency to organizations to pay the ransom — not only can they not operate as needed, but they may face regulatory fines and reputational damage if they “allow” sensitive information to be released.
- **Backups don’t cut it.** Cyber criminals know that many organizations rely on their backups to recover from a ransomware attack. Now, attackers access systems and install their ransomware, but they wait to make the ransom request, reducing the likelihood that a backup will eliminate the need to pay the ransom.
- **Cold calling.** Ransomware groups are now calling victims directly if they believe the organization is trying to restore from backups rather than paying ransom demands. A cold call makes a ransomware attack feel more personal and intimidating to victims.
- **Targeting backups.** Ransomware now targets backups directly. Most organizations pay the ransom in the hope that they can return to business, having relied on backups to protect them from a ransom-related attack.

**CYBER CRIMINALS
KNOW THAT MANY
ORGANIZATIONS RELY
ON THEIR BACKUPS
TO RECOVER FROM A
RANSOMWARE ATTACK.**



PREPARE FOR THESE 3 RANSOMWARE TRENDS

Paying the ransom is no guarantee

Given these changing tactics, many organizations are likely to pay demands for ransom, but that's no guarantee that they'll get their data, systems, or operations back. Some cyber attackers seek an initial ransom payment, and then return for more every few days. Other attackers sell the data they harvested, even after receiving the ransom.

Delayed encryption leads to more challenging attacks

Ransomware groups now favor "post-compromise" attacks, in which the threat actors wait to encrypt the data, first destroying backups and disabling security processes, gathering credentials, learning and modifying the target environment, and pulling out sensitive data. Then they launch an attack that's extremely difficult to recover from.

Ransomware attackers understand the value of data

Previously, ransomware attacks operated by denying an organization access to its own data until it pays the ransom, but ransomware developers have embraced the **value of data**. By making copies of the data and threatening to release it publicly, organizations face an additional threat. Not only are they unable to keep their organization free from ransomware, they may now be responsible for regulatory fines related to data protection. In addition, impacted organizations may lose customers, not only because their systems were down, but because customers no longer trust them.

Plan for ransomware

Cyber attackers made *at least* \$350 million in 2020, **according to Chainalysis**, so they aren't going to stop ransomware attacks in 2021. Don't wait until you get a ransom demand. Plan ahead so you can act decisively in case of an attack, and create a team that has authority to execute on large-scale, operational decisions to mitigate damages. Finally, consider possible vendor solutions and limiting users to the least privileged access necessary for them to do their jobs. Limiting access, together with monitoring, threat detection, and a response plan, can help you limit the amount of damage ransomware can cause in your organization.



"You think CrowdStrike's EDR will work with our Splunk?"

5 STEPS TO TURN YOUR MSP INTO AN MSSP

KATIE TEITLER

Managed service providers (MSPs) serve a critical function for businesses worldwide. With an estimated market size around the USD\$200 billion mark,ⁱ there is an obvious need for outsourced IT and operations support. More and more, however, companies cannot decouple security from IT, hence, the existence of managed security service providers (MSSPs). It's fair to say that a business could not use an MSSP without either running its own internal IT department or through partnership with an MSP. The reverse, however, is not true. Any business can have an IT function without a security function.

For the record, this is not recommended.

Clear bias aside, cyber security is intimately intermingled with all digital use and has become a top-line business priority for many organizations. A breach could bring devastating impacts to revenue, customer retention, future growth, reputation, and more. For this reason, many MSPs partner with MSSPs to offer customers the option of enhanced and dedicated security services. Yet, the estimated MSSP market valuation is ~USD\$30 billion,ⁱⁱ just a small fraction of the greater MSP market.

Why? Are companies, in particular, small and medium-sized businesses, just not deploying security technology? In some cases, the answer is yes. What we've found in our work with these smaller businesses via our [Cyber Corps service](#) is that it's easy for them to be overwhelmed with the idea of adding security. They know it's an important business decision, but they neither have the time nor internal resources to evaluate what they need. Oftentimes they rely on their MSP to make security recommendations, then they fear the cost of implementation and are thus stuck in a cycle of analysis paralysis.

Part of the problem is the business model; MSPs often rely on external MSSPs to deliver security expertise. This means that the MSP contracts with the MSSP on its own accord, offers security as a value-add to its customers, and passes along a cost plus a markup to the end customer. As a result, the customer pays a higher price for security services, but contracting on their own could be confusing,

THE OPPORTUNITY FOR ENHANCED SERVICES AND INCREASED REVENUE IS ATTRACTIVE TO THE MSP, AND IT BENEFITS THE END USER MARKET IN A VERY POSITIVE WAY.



plus there is no guarantee that their MSP would be able to integrate with whichever MSSP they choose. It's a circumlocutive cycle that hurts smaller businesses.

Partnering with a standalone MSSP is often not the answer, either, because most MSSPs have built their practice around the accepted current model and don't or won't offer some of the more basic IT functionality needed by these smaller businesses. It is easier, however, for an MSP to transform itself into a full MSSP, complete with basic IT services, by adding in-house capability. Over the last few years, we at TAG Cyber have seen this transformation occur within a not-insignificant segment of the market. The opportunity for enhanced services and increased revenue is attractive to the MSP, and it benefits the end user market in a very positive way.

Enterprising MSPs that want to take advantage of the need and opportunity can start with a few basic steps.

- 1. Strategy:** Unless your business is flush with capital (and kudos to you if it is) it will be impossible to incorporate full lifecycle security into your offerings immediately. Start by taking stock of what services you offer now, who your clients are, if there is a common thread to their security needs—e.g., they're all missing endpoint security or data protection—and how you can build or buy those capabilities first.
- 2. Technology:** Select the technology or capability you want to offer, then determine if its preferable to build, buy, or borrow (i.e., have a partnership agreement with a provider). Think carefully about the cost implications of each choice and the long-term impact on your business. While partnership agreements may be the easiest to execute, you will pay a higher price, and therefore have to charge a higher price, than if the technology is in-house.
- 3. Staffing and Training:** How will you accommodate 24x7x365 technical support (and potentially response capabilities when a security incident is discovered)? Can you hire and train enough security experts? Can you provide the ongoing skills advancement needed to keep pace with security demands? If the decision is to use third-party technology in your MSSP, how/when will the vendor supply training, for deployment as well as upgrades/updates?



"I thought we could use some cyber expertise on our board."

- 4. Integrations:** There is no doubt that some overlap exists between traditional IT and security technology. Today, many tools integrate via API, thus allowing operations staff simpler management and visibility. However, some legacy tools are harder to integrate, and some tech ecosystems just don't work well with others. Make sure that whatever tech you use, you aren't grappling with multiple, disparate systems and data streams, increasing the burden on your workforce and thus ratcheting up the potential for error.
- 5. Pricing:** One of the biggest advantages of the service provider model is economy of scale. The ability to use a centralized set of technology and staff across multiple customers allows for competitive pricing, but the tendency is to charge a premium for the security expertise brought to the table. Consider your target market before pricing your service out of reach. There is nothing wrong with charging premiums for expert-level work, but if the idea is to support smaller businesses, realize that the reason they're not already running a security program and security tools is because it's unaffordable to do so.

In short, upgrading your MSP to an MSSP is a great business opportunity. However, doing so requires more than just buying some new technology, deploying it, and offering it to existing customers. Develop a strategic, step-by-step plan, based on the needs of your current customers (and likely many others) that will help you grow, expand, and provide the necessary security capability so many businesses are lacking today.

i bit.ly/3bZ0ouK
ii bit.ly/3qU4zMM



7 TIPS FOR GIVING MEANINGFUL DEMOS

ADAM LEWINTER

Communicating the value of a security solution in a crowded and often homogeneous marketing environment is a real challenge. Sales processes are carefully calculated engagements, and the technical demo stage can often make or break an opportunity. In my career I have given nearly 5,000 technical demos in person, over video conference, or at trade shows. In building my craft, I have given both great and terrible technical demos (just ask any of my past sales reps for the horror stories). What I learned from it all is a set of principles that allowed me to communicate complex technical concepts most effectively and more often than not give a good demo.

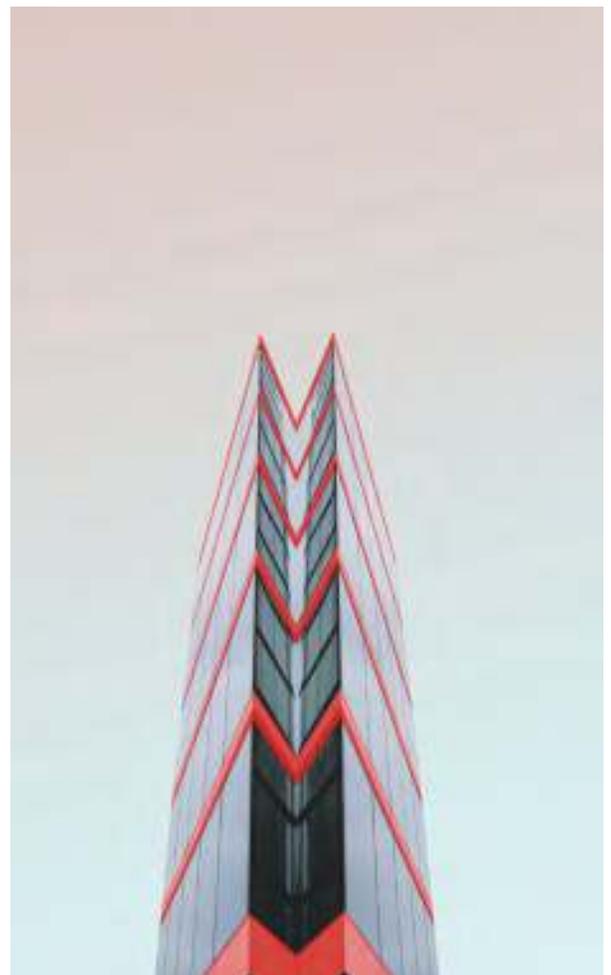
Now as an analyst, I find myself on the other side of the conversation with the fascinating new perspective of listening to complex technical concepts in which I have no expertise. Being an analyst has given me exposure to many different presentation styles that I would never have had the opportunity to experience as the presenter. Setting aside the fact I appreciate some styles more than others, the best demos I have seen all include the same principles I found from my years of presentations. Below is the list of the principles I have found to lead to successful technical demonstrations.

DEVELOP A COHESIVE NARRATIVE

The goal of a technical demo is to support the narrative you and your sales partner have been building from the first engagement. The demo is a story that acts as a visual aid to facilitate discussion or as the first step in providing proof for the claims in your sales pitch. The common mistake here is thinking that showing all the features of the product tells the story. Meandering feature tour demos are counterproductive and will at best lose the attention of the audience and at worst completely confuse the value proposition in the narrative.

Not to mention you don't have time to do a feature tour—you often have less than an hour to show your product, describe how it fits in their environment, address applicable uses cases, and answer any questions they have. Focus on the core aspects of the product that tell the story you want to tell.

THE DEMO IS A STORY THAT ACTS AS A VISUAL AID TO FACILITATE DISCUSSION OR AS THE FIRST STEP IN PROVIDING PROOF FOR THE CLAIMS IN YOUR SALES PITCH.



A good narrative addresses the business value of the product and should focus on answering questions like, “How will this make the job easier”, “How is this implemented”, and “How is this maintained”. At the end of the demo, a good narrative enables a technical champion to have personal investment in your product and management to see how it makes their team more efficient.

YOU CONTROL THE DEMO; THE DEMO DOES NOT CONTROL YOU

Your narrative should not be influenced by what is on the screen. Stick to your story and if the demo does not show it (because live demos will always have issues) then ignore what is on screen and keep to the story. There is no need to draw attention to issues or say “Oh, wasn’t expecting that”. This makes your product look immature, incomplete, or unstable. You should be able to be just as effective delivering the narrative presenting a blank screen than if you have a working demo.

BE CONFIDENT

Practice, practice, practice. If you are confident in your presentation you will receive less challenges to what you say (unless you are horribly off-base) and will have a stronger command of the conversation and message. Remove filler words like “um” and “uh”. Also remember that you are going to be the unchallenged expert in only one thing—your product. Know it well and know your click track so you don’t fumble around in a UI looking for something. Projecting confidence and competence is key when presenting concepts or ideas that might be new to the listeners.

BE HUMBLE

It’s easy to blur the line between confidence and arrogance. You want listeners to view you as an authority on the topics being discussed, but your goal is not to be the smartest person in the room. If you talk at a level over people’s understanding or degrade them, then they will ignore you and you will lose your ability to be a trusted advisor. No one wants to be made to feel small or unintelligent.

We have all been in situations where someone wants to be the smartest person in the room, and it is important to remember in this situation that no one wants to be challenged by a vendor. At best you look arrogant, at worst you build a detractor to your entire sales process. Keep control of the demo by acknowledging the points that are brought up and moving on. Oftentimes the points raised aren’t part of the problem the product is designed to solve, so it’s a perfect time to reiterate the purpose or primary goal of the product.

FULLY ADDRESS QUESTIONS

It’s imperative to always answer questions to the best of your ability, and it’s OK if the answer isn’t completely positive for your product. Admitting to shortcomings makes you more trustworthy and allows you to establish a role as a technical advisor. Perhaps most importantly, don’t be afraid to say, “I don’t



know.” You won’t know everything and will often present to people who know more than you and are smarter than you. That said, it’s very important to follow up with the answers once you are able to find them after the demo. This provides a perfect opportunity for another touch point to continue the conversation.

It’s also a good idea to ask clarifying questions as needed. Asking why something is important or what the reasoning behind a question is often reveals preconceived notions that someone has that may be addressed in a different way than they are used to in your product.

KEEP IT INTERACTIVE

No one wants to be lectured. You might also be presenting concepts that the listener has not considered before and needs time to digest. Don’t just plow through the words of your story. Pause after particularly technical or conceptual points to allow the listener to digest and ask questions. Prompting your audience for questions allows you to address any confusion and ensures they are following your story. Perhaps most importantly, leave time for discussion. Post demonstration discussions allow you to uncover requirements that will allow POCs to be completed quickly and without issue or address any remaining barriers to progressing the deal. Remember that time is extremely valuable, and you may not get another opportunity with your audience to get this information.

BE ADAPTABLE

If you keep getting the same questions each presentation, adjust your narrative to address them. Even if it is an objection, if you address it first, you control the narrative around it and won’t seem as defensive as when you wait until the prospect brings it up. Also pay attention to areas that might be harder for the audience to accept or digest. Removing objections brought up by listeners by preempting them in your narrative will also lead to an overall positive feeling about your product to the listeners.

SIGNS YOU ARE SUCCESSFUL

Having a way to measure success is just as important as developing the skills. You know you are successful in your demo if you stop getting questions about how the product works and instead get questions about solving particular use cases. This means the listener has bought in to your narrative and approach and is now looking for ways to use it in their job. This should not be mistaken as a closed deal, but you have succeeded in the purpose of a demo if they understand what your product does and begin to think how it would apply to their specific problems.

The key takeaway should be that the technical demo is not about showing how well designed or engineered the product is. Rather, it is there to show how the product solves a problem. This nuance is extremely important and is often at the core of what determines a good versus a bad technical demonstration. The common misconception is that the product will sell itself and sales will be generated by just showing how well it is built. However, you can have the most well-built and clever product ever to be designed but if the prospect doesn’t see how it solves a real need, you’ll never make a single sale.

NOTE TO CYBER STARTUPS: THE FIRST \$3M IS THE HARDEST

EDWARD AMOROSO

One of my favorite books from the Awesome Eighties was *Getting by on \$100,000 a Year (and Other Sad Tales)* by business writer Andrew Tobias. The implication of the book's title, coined four decades ago, was that a hundred-K should be an impressive enough salary to keep even the toniest Upper West Side Yuppies pretty well fed. We all remember, however, that for many of the spoiled brats from that era, \$100K was just not enough to get by.

I mention this book and the whole 100K-thing not because it has anything to do with cyber security or with modern startups, but that it has everything to do with the challenge of using absolute numbers in any estimate. You can see from my title that I am going to make a special fuss about three million dollars – and as I type the words, I can feel the embarrassment of reading this in 2061. (Note to future self: I hope \$3M is still a nice take.)

That said, I have come to the broad conclusion, based on having reviewed thousands of cyber security startups over the past five years as a TAG Cyber analyst, and prior two decades as the CISO for a Fortune 10 company, that when a startup reaches \$3M in annual revenue, it can take comfort in the fact that it will likely have the ability to go to much higher levels of business. Let me explain why I picked that number – and why my conclusion should hopefully resonate.

Cyber security analysts (and anyone else working in an analytical field) take on complex problems by breaking them into smaller pieces. We thus analyze companies by breaking them into the constituent pieces that support their mission. This might involve three product lines, or perhaps a pipeline of development, marketing, and sales. It can also involve professional support for one or more major customers.

But in every case, when we look at a startup company, we always want to see evidence of meaningful revenue, with a high chance of recurrence, and with sufficient customer diversity to protect against unexpected business cycle bumps. We've learned that \$3M in revenue is good

evidence of all three requirements. Interestingly, we've not seen this target threshold differ much in importance between services, products, and platforms.

Let's start with meaningful revenue. What we mean here is that the start-up should have enough paying customers to support a reasonable portion of their operations. Whether well-funded by venture capitalists, guided along by a rich angel, or bootstrapped through sales (healthiest case), a company generating \$250K every month from sales enjoys a stable, ongoing base for dozens of salaries and non-trivial platform investments.

WHAT WE'VE NEVER SEEN, HOWEVER, IS A STARTUP WITH ONLY ONE CUSTOMER PAYING \$3M. THIS LEVEL OF REVENUE ALWAYS DICTATES A DIVERSITY OF PAYING CUSTOMERS – WHICH IS VITAL FOR SUBSEQUENT GROWTH.



Next is recurring revenue. Startups would like to see general revenue trending upward, but all will experience the normal ups and downs of the business cycle. If a start-up has \$1M in revenue, then danger exists that it can easily swing temporary to zero – and this calls into question viability, as well as willingness of investors to stick with a company. At \$3M, however, the normal cycle-based swings will keep things comfortably away from zero.

Finally, there is customer diversity. Cyber startups sometimes get lucky and pick up a customer who is willing to try out their platform. We've seen these engagements range from tiny one-time payments for POCs to higher, ongoing fees for a larger relationship. What we've never seen, however, is a startup with only one customer paying \$3M. This level of revenue always dictates a diversity of paying customers – which is vital for subsequent growth.

Take for example the demo mirage. We often see tiny startups with ten or more fancy logos of Fortune 50 companies. They tout these engagements as evidence of massive potential growth. But we know that big companies are usually nervous about deploying goods from little companies into production. So, they often do a paid \$100,000 POC. A startup would have to do 30 of these to hit \$3M, so again – that threshold requires more than just POCs.

Look – I understand the somewhat arbitrary nature of \$3M as a revenue target. And I understand the arithmetic of the well-funded stealth operation with little or no revenue that unveils to high demand and skyrocketing growth. But these are exceptions. Stealth teams eventually must make money, and just as Houston relaxed when the shuttle cleared the tower, investors should feel good once their investment has hit \$250K per month.

For those of you who have cleared this goal – nice job. Now it's time to vault Geoffrey Moore's famous chasm. But for those of you still driving toward this objective, I can offer this: You will find that once you pass the magic number, subsequent growth will be easier. Mind you – this does not imply that it will some lay-up. It just implies that it will be easier. Companies in this category should agree: For cyber security startups, the first \$3M is the hardest.



THE GROWING OBSOLESCENCE OF CREDENTIALS

JAMES ROUTH, *GUEST AUTHOR*

Back at MIT in 1960, Fernando Corbato developed the password while establishing the Compatible Time-Sharing System (CTSS), enabling file permissions to registered users. Sixty years later, user IDs and passwords have served enterprise security remarkably well. Credentials (user IDs and password combinations) remain the predominant method for enabling online authentication today on the vast majority of websites, mobile applications, and Software as a Service (SaaS) applications. Many cyber professionals advocate for increasing the strength of passwords (more complexity, upper-lower case, special characters, lengthy phrases, etc.) to improve the effectiveness of passwords as an authentication mechanism.

We're now facing a new reality where the use of passwords as an effective authentication method has changed. The reality for enterprises today is that the use of passwords as an effective authentication method is growing in obsolescence and the primary reason is how they are being applied to multiple web sites and mobile applications.

Most digital consumers have more than a hundred websites, SaaS, and mobile applications that require unique passwords, and remembering the credentials for each website or mobile application is directly related to how often the website or mobile app is used. The enterprise wants frequent interaction, so the opportunities for an increase in brand awareness increases. The digital consumer wants convenience and easy access to their data. Consumers re-use passwords across sites to reduce the number of passwords necessary to remember. The inherent problem is not necessarily with the credential itself but rather how it is being used (or re-used) by consumers across digital assets.

The most effective way to understand this growing obsolescence of credentials is to look at the perspective of a cyber criminal. Over the past five years, cyber criminals figured out that it is easier to use credentials to hack into systems rather than exploiting vulnerabilities in hardened systems. The tools and credentials available to threat actors enable them to use automation to take over online accounts at a scale with few constraints.

TECHNICAL SKILL IS NO LONGER A PREREQUISITE FOR THE CYBER CRIMINAL WHO SEEKS ONLINE ACCOUNT ACCESS USING ACTIVE CREDENTIALS. THEIR FIRST STEP IS TO ACQUIRE CREDENTIALS (USER ID AND PASSWORDS) IN BULK THROUGH FRAUD FORUMS ON THE DARK WEB IN EXCHANGES WITH OTHER CYBER CRIMINALS.



Technical skill is no longer a prerequisite for the cyber criminal who seeks online account access using active credentials. Their first step is to acquire credentials (user ID and passwords) in bulk through fraud forums on the dark web in exchanges with other cyber criminals. There are billions of credentials available. The second step is to use a tool like Sentry MBA (a commercial software product designed to enable individuals to initiate authentication attempts at scale on websites of their choosing) to try out the credentials on active websites. This typically results in a 2% success rate due to the increasing use of the same password across multiple sites by digital consumers.

If a criminal has access to 10,000 of the billions of credentials available on the dark web and chooses to use an automated tool for applying the credentials to websites, it can yield ownership of 200 online accounts. That enables their access to account information and monetizing it through downstream fraud tactics (aggregating the data and offering it for resale,

setting up linkages to money-mule accounts, or making fraudulent purchases). This approach is called “credential stuffing” since it uses credentials in bulk. There are billions of credentials available with few constraints to cyber criminals using active credentials to commit fraud.

Enterprise systems have been using credentials as a primary authentication technique based on the fundamental premise that the enterprise user or consumer is the only one who knows the credentials, thereby making this an effective technique for determining the identity of the user/consumer. All IT professionals were taught that online authentication is an event with a beginning and an end. The outcome of the authentication event is always binary, meaning successful access to the system or no success at access. If access is enabled, then the digital user is trusted with the account information and transaction capabilities provided in the application. If authentication fails, then access is not enabled, and the user/consumer is no longer trusted with access to functionality of the application.

As a result, cyber security professionals today consider adding binary authentication techniques to credentials to improve the effectiveness of authentication using several factors most often called multi-factor authentication, or MFA. The working premise of using MFA is that if the credentials are compromised, the system can rely on a second factor before granting access to the application. If the user ID and password are compromised, then the second factor will provide the necessary authentication factor. The consumer has to remember how to enter the user ID and password combination while then receiving a one-time password (OTP) sent through text message, for example, and how to enter the OTP in the website login page to obtain access. This approach adds friction to the threat actor that was able to obtain the active credentials and results in more effective security and risk management. This approach, however, also adds friction to the digital consumer or enterprise user.

There are alternatives to consider for MFA options, but for most enterprises these options are designed to fit into the construct of an authentication event. Binary authentication techniques can be defeated by threat actors. The addition of a factor makes it more difficult for the threat actor/cyber criminal while also creating friction for the digital consumer. Cyber professionals believe the consumer friction is simply part of the cost of protecting sensitive consumer data. Cyber professionals consistently consider MFA options that represent trade-off decisions between digital friction for the consumer versus the threat actor based on the sensitivity of the data at risk. Highly sensitive data requires more friction. Less sensitive data requires a lower level of friction. Cyber professionals are asked to “facilitate” the trade-off decision process for determining the tolerance for consumer friction necessary for protecting the level of sensitivity of the online data. As a board member, you have an opportunity to encourage management to consider password alternatives that reduce consumer friction while improving risk management.

Enterprises that accept the need for consumer friction and implement an MFA approach recognize that large percentages of online consumers choose not to adopt the MFA option and avoid use of the online capability. Many try to use the MFA capability and give up during the registration process, opting to simply

reset their password on the few occasions when they need to use online functionality. The consumer experience of friction is not worth the benefits of online functionality to them. In some cases, enterprises see 30–50% of digital consumers avoid the friction of MFA options, opting out of or avoiding account registration.

Estimates of web traffic from criminals attempting authentication for popular consumer digital sites is upwards of 50–90%. That means that if an enterprise is highly successful and cultivates a digital brand for consumers, then the majority of web traffic hitting their load balancers and web application servers is from criminals attempting to steal customer data. A large and growing percentage of an enterprise's IT infrastructure cost for digital assets is subsidizing criminal web traffic attempting authentication on their systems. The simple economic viability of this model is not sustainable for any enterprise over time. The cost of providing digital capacity to criminals is not in the shareholder's best interest. Credential theft is the heart of the problem.

ACCOUNT TAKEOVER IS NO LONGER FEASIBLE SINCE THERE ARE NO MORE CREDENTIALS TO BE COMPROMISED. DIGITAL EXPERIENCE IS IMPROVED FOR THE CONSUMER SINCE THERE IS NO NEED FOR PASSWORDS.

An easy way for you to understand how widespread the use of credential stuffing by threat actors is to do a search for the number of YouTube videos available to demonstrate how to use Sentry MBA for credential stuffing (over 200,000). That is an indication of how widespread credential stuffing is as a tactic; there are thousands of videos with the same purpose – to teach criminals how to perform credential stuffing attacks.

A few enterprises that have dealt with the practical challenges of MFA implementation along with the resulting consumer friction are attempting to fundamentally change the rules for enterprise authentication for the next sixty years without relying on credentials. The potential results for these enterprises include:

1. A digital consumer experience with significantly less friction (no passwords to remember)
2. A fundamentally more effective method of online risk management that reduces account takeover
3. A lower operating cost model that eliminates the need for password reset

Better online security with less consumer friction at a lower cost sounds too good to be true. I don't understand why more enterprises are not applying this model today. It is not because the technology does not exist; there are enterprises that have this in production and have recognized the benefits for several years.

What I am certain of is that for an enterprise to consider a model that reduces consumer friction while improving security at a lower operating cost, they must come to grips with their ability to un-learn something foundational in the definition of enterprise authentication. IT professionals were taught that authentication was an event with a beginning and an end. The outcome was binary, success in gaining access or not. Adding binary authentication techniques to an authentication event always results in additive consumer friction, and there are always ways to break it for a threat adversary.

Considering authentication as a continuous process instead of an event changes the paradigm and opens up whole new possibilities. For example, an enterprise can capture online behavioral attributes from the consumer and develop a pattern of behavior for that specific attribute represented as a number or algorithm (mathematical representation of an event). This becomes a baseline reference for

then capturing the attribute data in real time during a web or mobile session and comparing it to the baseline or pattern. This results in a deviation score for that attribute at that point in time. Combining this with many deviation scores from multiple attributes can be represented by a single aggregated score that determines a confidence level. That confidence level score can be fed to any application in real time to enable it to take action within specific and predetermined threshold levels. If the confidence level is high, then full access to the website functionality is provided. If the confidence level dips beyond a predetermined threshold, then access is restricted. The single confidence score (or deviation score) can be used by multiple applications with different actions or consumer treatment options based on the sensitivity of the data.

All of this can be performed without any action taken by the digital consumer so they don't experience friction. Consumers can choose their method of choice for authentication when they purchase and set up their cell phones, laptops or tablets. A standard is used across manufacturers called FIDO 2.0, agreed on by device manufacturers and carriers, enabling iPhone consumers to select authenticators (Touch ID, Face ID) and Android consumers to select fingerprint authentication using the FIDO 2.0 standard. The fingerprint never leaves the device and is protected, but a validation is confirmed using the FIDO 2.0 standard (WebAuthN). This way the digital consumer chooses their authentication approach, and this choice is incorporated into the continuous behavioral based authentication model of the enterprise.

Account takeover is no longer feasible since there are no more credentials to be compromised. Digital experience is improved for the consumer since there is no need for passwords. No more help desk calls to reset passwords means lower costs.

The same continuous behavioral based authentication model will work across channels (web, mobile, voice) offering better risk management and consumer digital experience enabling the consumer to have choices of channel and authentication experience.

Today there are many alternatives to using passwords for authentication and many vendors promoting their use of "passwordless authentication." These types of solutions represent a positive step forward toward a better authentication experience and should be considered within the context of improving the digital consumer and user experience.

Is your enterprise considering a strategy for eliminating credentials today? It may be a good time to ask management why they are not considering evolving their digital authentication strategy to improve the consumer experience with better security and a lower cost.

Sources:

www.en.wikipedia.org/wiki/Credential_stuffing
www.blog.shapesecurity.com
www.akamai.com/us/en/infographics/credential-stuffing-the-risk-of-bots-to-your-business-infographic.jsp
www.welivesecurity.com/2019/04/10/credential-stuffing-attacks-login/ https://owasp.org/www-community/attacks/Credential_stuffing
www.darkreading.com/attacks-breaches/credential-compromises-by-the-numbers/d/d-id/1333733
www.blog.barracuda.com/2019/04/02/is-2019-the-year-credential-stuffing-dominates-the-threat-landscape
www.imperva.com/resources/resource-library/reports/2020-bad-bot-report
www.bleepingcomputer.com/news/security/28-billion-credential-stuffing-attempts-during-second-half-of-2018
www.medium.com/@josefinablattmann/8-alternatives-to-conventional-passwords-you-need-to-know-aea5bfe296
www.swoopnow.com/password-alternatives
www.synopsys.com/blogs/software-security/password-alternatives
www.bbvaopenmind.com/en/technology/digital-world/digital-security-5-alternatives-to-passwords
www.entrepreneur.com/article/309054
www.welivesecurity.com/2015/02/05/alternatives-passwords
www.thenextweb.com/podium/2019/06/21/alternates-to-passwords-11-ways-to-safeguard-logins-to-websites-or-programs

A NEW PROGRAM ASSESSES LAW FIRM SECURITY

DAVID HECHLER

Data breaches at law firms have made headlines in recent years. The [Panama Papers scandal](#) in 2016 led to the demise of the Mossack Fonseca firm two years later. The 2017 ransomware attack that [shut down DLA Piper](#) brought the message home. And the attack last year on New York's law firm to the stars, [Grubman Shire Meiselas & Sacks](#), seemed to underscore the point.

But law firms have been slow to respond. And perhaps more surprisingly, so have the companies that hire them. A 2019 survey conducted by the Association of Corporate Counsel (ACC) found that 70 percent of the in-house counsel who responded said their companies had not attempted to assess the security of the law firms they'd hired. Many of these companies routinely evaluate the security of their other vendors, but somehow they'd missed the boat on their law firms. Even though these firms possess some of their most sensitive data.

Late last year ACC launched a business to address this security hole. They call it the [ACC Data Steward Program](#) (DSP). It's specifically designed for corporate law departments that want to ensure their firms protect their data—and for law firms that want to showcase their security.

Jim Merklinger, president of the ACC Credentialing Institute, described the new program as a “win-win” for law firms and their clients. The program aims to replace the security questionnaires companies often send vendors. Generic questionnaires have never worked well for law firms, Merklinger said in an interview, because the questions are not designed to apply to their specialized tasks. The result is that many of the questions come back marked “not applicable,” he noted. And often there are hundreds of questions—sometimes more than 1,000. And no two questionnaires seem to be alike, placing a great burden on the firms.

The DSP was designed to streamline the instrument into a standardized, automated format that allows law firms to self-assess their security and make the results available to as many clients as they wish. Merklinger and his colleagues, working with an advisory group of law firms, legal service providers, and in-house counsel, winnowed the questions to 160 controls. They're based on categories and content pulled from the [NIST Cybersecurity Framework](#). The firm completes the form by choosing multiple choice answers that describe its own policies, procedures, processes, and expertise. When the form is complete, the firm is given a rating (100 is perfect).

THE COSTS

The standard package costs \$9995 a year. This allows the firm to share its results with as many clients or prospective clients as it chooses. The service never shares the data with anyone, Merklinger emphasized. It's completely up to the firm. This fee allows the firm to update any information during the year at no extra charge. For instance, if a law firm adds multifactor authorization to some of its processes, it can add that

THE ASSOCIATION OF CORPORATE COUNSEL DESIGNED A WAY FOR LAW DEPARTMENTS TO EVALUATE OUTSIDE COUNSEL.



information and improve its rating. Also, if a firm wants to highlight for a client certain capabilities that are not included in the standard controls, it can add its own items into the mix and share these with specific clients at no extra charge. (These would not, however, change the firm's rating.)

There are two alternatives to the standard program. If a law firm has only one client that wants to see an evaluation, it can pay \$1495 a year for the single-client option. That's the bare-bones offering. Suppose a firm wants to go the other way? If it wants its security prowess certified by an independent third-party expert, the DSP also offers that. The firm still has to pay the annual fee and complete all the information required on the standard package. It then pays an additional \$8000 once every three years for the independent certification. And, of course, it must respond to all of the questions and requests from the independent assessor.

THE ROLE OF THE LAW DEPARTMENT

Corporate law departments are not charged any fees. ACC hopes that they will see the benefits and encourage their firms to sign up. That would relieve legal departments of the responsibility of finding or creating a security questionnaire, and provide them with a wealth of information about their firms.

The information goes far beyond the equivalent of a grade on a test. The ratings are just a snapshot, Merklinger said. Law departments can dig into the results by accessing the DSP assessment's dashboard. There they see the firm's strengths and weaknesses. And how they answered each question. They can also input requests for evidence to back up the firm's answers. The program makes it easy for the firm to respond to those requests by uploading spreadsheets, screen shots, or other relevant documents.

The biggest surprise so far, Merklinger said, is that law firms have become "big proponents of this." It's a way to demonstrate their strengths. This may be particularly appealing to some small firms, he said. He cited firms that are part of the **NAMWOLF** network as an example. The assessment can also help firms see areas where they need to improve. It may even spur conversations with their clients about steps to remediate deficiencies.

With all the examples of breaches at law firms, Merklinger thinks he's got the right product at the right time. The program got rolling late last summer, he said, and he hopes that by the end of 2021 they have 300 firms on board.

At the end of the interview, Merklinger conjured a conversation between a general counsel and his CEO. They've just learned that they've had a data breach. "This information got out from the law firm we hired," the CEO says to his top lawyer. "How did they do on the evaluation we gave them?" The general counsel hesitates. "We didn't evaluate them."

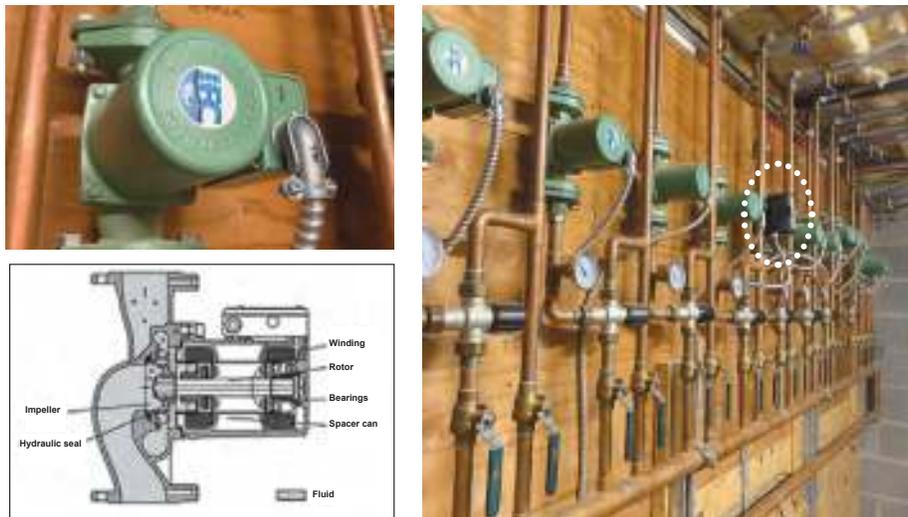
"I would not want to be that general counsel," Merklinger said.



"Dad, tell me the one again about the cool IT manager who saves his department from ransomware!"

WANT TO STOP NATION-STATE CYBER THREATS? SIMPLIFY.

ED AMOROSO



John Von Neumann once made the following assertion: For small mechanisms, it's easy to see how they work, but not what they do. In contrast, for large systems, it is easy to see what they do, but not how they work. Based on nearly forty years in cyber security, I've come to view this as the central challenge in securing large-scale systems: We know what our systems are intended to do, but we don't have a clue how they actually work.

Look at the pictures above. The simple mechanism on the top left is a pump that drives the radiant heat in my home. One of these pumps recently broke and the repairman came and replaced it with a newer model (circled in the diagram on the right).

When asked how the pump works, the repairman described it perfectly and completely. A quick Google search offered a simple diagram (see picture in lower left) that confirmed the explanation. The newly installed pump worked the same but had more umph.

When asked how the overall system worked, the repairman can explain the system from end-to-end in great detail. My wife (no technical or plumbing background) also has come to understand the system and often diagnoses issues perfectly and accurately.

If you do enterprise cyber security for a living, and you are wondering what the goal of our profession might be, I offer the above plumbing use-case as exemplary. When we can point to a component and understand it completely, upgrade or replace it trivially, and then get back to other matters, we will know that our profession has arrived.

Now a test for you: If I asked you to show me how your IAM works in the context of your overall cyber security scheme, could you do it? Or how your cloud container security orchestration works? Could you do it? Do you have a detailed and accurate diagram?

If you are honest, then I suspect you will understand the task at hand – and will get to work at once with this: You must demand simple components, and you must fight to urge to accept additional complexity. If you cannot explain it and diagram it, then it's too complex.

That is the secret to securing your infrastructure.

The background of the entire page is a grid of dark, thin lines forming a pattern of squares. Each square contains a distorted, blue-tinted reflection of a modern building's facade, likely a skyscraper with many windows. The reflections are mirrored and slightly warped, creating a complex, abstract pattern of light and dark blue tones. The overall effect is that of a multi-layered, digital or architectural visualization.

INTERVIEWS



Dubeau

AN INTERVIEW WITH MONICA DUBEAU,
DIRECTOR, PRIVACY & CYNTHIA LUU,
PRODUCT MARKETING MANAGER, IBM



Luu

DATA GOVERNANCE AND DATA PRIVACY: SOURCES OF BUSINESS GROWTH

With GDPR and CCPA staking data privacy as widespread legal mandates, you wouldn't be alone in thinking that privacy is yet another compliance requirement you must address. These might be the biggest and most well-known regulations, but they are far from the only ones you need to pay attention to.

If you're reading this Quarterly, this is no surprise.

However, on the coattails of compliance, data privacy and security have become more than mere laws and regulations. The ability to demonstrate the security and privacy of customer, partner, and employee data is a competitive differentiator in an age when breaches are rampant and attack surfaces are huge.

IBM Security, a lesser known but nonetheless formidable player in the privacy space, has been building products to help companies manage data and privacy for years. Given their reputation as a powerhouse, we recently spoke with Monica Dubeau and Cynthia Luu from IBM's security and privacy teams about their views on privacy protection.

TAG Cyber: What are the top privacy concerns of the enterprises and CISOs you work with?

IBM: We hear from our customers every day how challenging it can be to keep pace with a world where more and more data is being collected and shared across the hybrid multi-cloud environment. Businesses want to take advantage of their data to unlock value with analytics and AI, but safely sharing that data can be a roadblock in a reality where breaches occur frequently and protecting that data is often stymied by manual processes and disjointed tools.

Maintaining the privacy and security of that data can be a formidable task for any seasoned security leader. And today's consumers are a lot savvier and more aware of and concerned about the widespread use of their data. In response, data privacy regulations—GDPR and CCPA being top of mind—are growing in scale and complexity. We often hear from customers about their concerns with balancing how to drive business outcomes with data and providing transparency on how that data is being used.

At IBM Security, we believe that businesses do not need to consider a trade-off between preserving data privacy and growing the business—you can turn data privacy into a source of differentiation and business growth.

TAG Cyber: For enterprise security practitioners, what are the substantive differences in attitudes toward data privacy in varying geographies?

IBM: Wherever you are in the world, you cannot address data privacy without data security, and we find that the organizations we work with

Part of that value is knowing that the business is respecting customer data by providing transparency on how that data might be used and applying appropriate security controls.



are prioritizing both. Many major markets and countries have a privacy regulation of some level of maturity at this point, and as a result, businesses are prioritizing data privacy and regulatory compliance across the board. It is simply the cost of doing business in today's interconnected world.

Where there may be differences in attitude is based entirely on whether there has been a long-standing data privacy law in a certain geography. GDPR came into effect in 2018, but even long before, there were various privacy mandates and cultural influences that made personal privacy a priority. So for a business based in Europe, they most likely already have a mature privacy program and are looking for ways to optimize their privacy operations. From the CISO to the marketer, privacy is highly integrated in how they do business.

Contrasting that with geographies like North America that have more recently passed data privacy regulations, businesses that are not truly international (and may not have been pushed to develop a privacy program by foreign privacy legislation) are playing catch-up. They often see privacy as a hurdle that will require substantial investment. To them, data privacy is another challenge to address, rather than a way of life.

TAG Cyber: Companies rush to collect and use as much data as possible—to service customers, to identify business opportunities, and to generally grow business. Is this focus on data collection and use at odds with the ability to protect it?

IBM: Absolutely not. At IBM Security, we believe that with good data management and governance, coupled with data security, your data should be a source of business growth. Oftentimes, customers willingly share data to help the brands they enjoy provide better, personalized services. But this will only remain true if the value exchange is equitable between the business and the customer. Part of that value is knowing that the business is respecting customer data by providing transparency on how that data might be used and applying appropriate security controls. Data privacy can be a competitive differentiator because, more and more, customers are choosing brands based on data policies and companies that go the extra mile in respecting their data.

TAG Cyber: What are the components of the IBM privacy framework?

IBM: IBM Security believes that businesses can drive outcomes with a holistic and adaptive approach to data privacy based on zero trust principles and proven security solutions, connected on an open platform. We help accelerate your ability to deliver trusted customer experiences with unified security and privacy



workflows. Our framework is simple, and it keeps the customer and their data at the center of any organization's data privacy practice, which should demonstrate transparency and accountability at every phase. These phases include:

assessing data usage and risk against customer and regulatory responsibilities, protecting personal data with security controls, and responding efficiently to remediate risk and compliance issues. Businesses should expect to revisit these phases continuously and dynamically adjust to new customer demands, changes to the data, and more complex privacy regulations.

TAG Cyber: What are a few things companies can do immediately to up-level their data privacy protection, even if they cannot buy and deploy a privacy solution?

IBM: Privacy is a team sport, and one of the ways companies can set themselves up for success is to put together a cross-functional team of executives, line of business leaders, and other stakeholders, to agree on a data privacy vision and collaborate on a privacy standard on how to handle personal data internal and external to the organization. This is an exercise of leadership and team management, but a necessary step to start the process of improving data privacy protection.

These days, it seems like security and privacy leaders are being asked to do more with less budget. Luckily, privacy and security require technologies that overlap, which makes for a better investment justification. Obviously, the overlap isn't complete, but security provides the supportive underpinnings for handling and processing personal data that is essential for delivering trusted customer experiences and respecting privacy. If you have a tool that discovers and classifies sensitive data, see if you can extend that to assess for personal, regulated data. Same for any data activity monitoring tool, encryption technology, or solution for controlling user access—all capabilities that help address privacy needs. So, take a hard look at your existing tools and see if they can be extended to better accommodate for data privacy uses.



AN INTERVIEW WITH CANDID WUEST,
VP OF CYBER PROTECTION RESEARCH, ACRONIS

A HOLISTIC APPROACH TO INFRASTRUCTURE, DATA, AND DEVICE CYBER PROTECTION

The Holy Grail of cyber security is full lifecycle management. Workloads must be protected from the instant a user or system is connected, a piece of data is created, or a new tool is made operational, all the way through to data destruction or removal and instances when a compromise or breach occurs.

Most enterprises use disparate tools, techniques, and processes for each lifecycle stage. It's why there's an abundance of security vendor technologies available on the commercial market. And vendors have gotten savvy; most recognize the requirement for inter-technology compatibility. Thus, even if a vendor builds and sells a capability to address only one lifecycle stage, it often integrates with other best-of-breed technologies to give customers holistic visibility, orchestration, and governance.

Acronis, a well-known data backup and recovery provider, has pivoted on their strategy and technology. We recently spoke with Candid Wuest, VP of Cyber Protection Research at Acronis, about the philosophy of cyber protection and how it enables businesses to comprehensively protect their data and systems.

TAG Cyber: Traditionally, data protection and backup were separate and distinct IT functions from cyber security. Why is this an outdated approach?

ACRONIS: Cyber threats have evolved over the past few years and will continue to do so into the future. We've seen that attackers are combining different methods to compromise machines, steal data, or otherwise disrupt businesses. It is therefore vital to take a holistic approach to protection, one that can cover the whole organization—infrastructure, devices, and data—in all situations. For example, imagine a targeted ransomware attack, which nowadays often tries to delete existing backups as well as steal sensitive information before encrypting critical workloads or files. To protect against such a multi-pronged attack, you need to break the silos of backup and cyber security. For ransomware attacks, this means you need to protect the backups from tampering in order to ensure that you can recover a clean copy, should there be a compromise.

TAG Cyber: Why and how did Acronis decide to expand the range of products and services you offer?

ACRONIS: Over five years ago, Acronis began observing more and more of our customers suffering from sophisticated ransomware attacks, destroying their backups and fast recovery capabilities. On this premise, Acronis developed a threat-agnostic data protection technology called Active Protection, which monitors any data interaction on a system and uses artificial intelligence to separate legitimate activities from malicious ones. Since Acronis has granular data backups, we can restore

With some of these attacks yielding millions of dollars in ransom, there's no reason for threat actors to stop.

damaged or encrypted data in the event of a compromise. All of this functionality is provided from within a single agent, allowing the system to automatically restore without the need for user interaction. For example, if a previously unknown ransomware variant manages to encrypt a handful of files, the heuristic will automatically detect this tampering, stop the process, and restore any modified files.

TAG Cyber: Why is Acronis' legacy as a backup and recovery provider an important underpinning of Acronis Cyber Protect, your new solution?

ACRONIS: Building on the success of the integrated Active Protection and backup, Acronis decided that an adequate cyber protection solution needs to be built across even more domains. For example, it's important to address the five vectors of cyber protection—availability, accessibility, privacy, authenticity, and security (SAPAS)—which cover the full lifecycle of data. This is why Acronis integrated backup and a full next-generation security solution into a single agent, which has become Acronis Cyber Protect. This includes cloud-based reputation, signature-based antivirus, and AI-based pre-execution scanning. On top of this, the behavior of every running process is analyzed in real time, allowing cyber analysts to react to unknown threats at any stage. In addition, URL filtering prevents users from reaching malicious websites such as phishing websites, minimizing the risk of further attacks.

To cover all five stages of the NIST cybersecurity framework, the Acronis Cyber Protect solution also includes vulnerability assessment, patch management, and exploit prevention functionalities, which help prevent attacks from succeeding in the first place. At the other end of the NIST framework, in the “recover” phase, our forensic data backups allow a thorough root-cause analysis that provides richer data than traditional EDR.

TAG Cyber: What are some of the bigger or more recent threat trends you're seeing?

ACRONIS: One of the biggest threats against organizations of all sizes is targeted ransomware. Modern ransomware attacks not only encrypt data, but also steal sensitive information and disrupt business operations with distributed denial of service (DDoS) attacks. These attacks will continue to grow in number—cyber criminals are increasingly automating their attacks and even starting to use AI to increase their success rate. With some of these attacks yielding millions of dollars in ransom, there's no reason for threat actors to stop. This means that there is a need for integrated and automated solutions that can handle the full scope of these attacks.



Another threat that has increased drastically during the COVID-19 pandemic is phishing attacks, leading to a rise in compromised credentials. In February 2021 alone, we observed over 700,000 malicious requests. User awareness training programs can be as good as they come, but they are never 100% effective; there will always be at least one user who clicks on an enticing or confusing link, and therefore enterprises need a technical solution to protect against phishing.

TAG Cyber: What types of clients are onboarding to Acronis Cyber Protect?

ACRONIS: There are two answers to this question. First, Acronis' go-to-market strategy is primarily channel-focused, enabling services providers of all sizes and types (MSPs, telcos, hosting companies, etc.) to offer cyber protection services to their end customers. We have an existing partner network of over 50,000 channel partners worldwide, and we're encouraging them to build new cyber protection services by leveraging our Acronis Cyber Protect Cloud platform. Installed via one agent and managed through one central console, our service provider platform integrates cyber security, data protection, and endpoint management in a single solution that protects endpoints, systems, and data. The essential capabilities include full-image and file-level backup and recovery for workloads on more than 20 platforms; an advanced AI-based behavioral detection engine that stops malware, ransomware, and zero-day attacks on client endpoints; and centralized management that integrates with remote monitoring and management and professional services automation systems.

Vulnerability assessments, file sync and share, blockchain-based notarization, and disaster recovery are also included and available as add-ons.

Our second (but equally important) target market is the ultimate end user. Service providers primarily cater to the small and medium business (SMB) market. SMBs generally do not have the resources or expertise to handle their basic IT environments, let alone triage cyber threats, so they rely quite heavily on service providers to do this for them. Ultimately, Acronis' solutions are being consumed primarily by SMBs but they are being delivered by service providers.



AN INTERVIEW WITH GAURAV BANGA, FOUNDER AND CEO, BALBIX

ARE YOU BLIND AND EXPOSED TO TOO MUCH CYBER RISK?

The enterprise attack surface is already massive and expanding continuously, introducing new risks and threat vectors which enterprise security teams must be aware of and prepared to mitigate. Between weakness in infrastructure, applications, endpoints, IoT, the supply chain, and more, it's hard for security professionals to quantify their company's cyber risk. However, more and more, executives and boards of directors are demanding insight into how their cyber security program is faring and how they can avoid breaches.

Unfortunately, analyzing and improving (i.e., decreasing) cyber risk is no longer human-scale manageable. Millions of continuously changing signals need to be analyzed, correlated, and prioritized for investigation and mitigation.

The key to decreasing cyber risk, says Gaurav Banga, Founder and CEO at Balbix, is automating the pieces of cyber security posture management controlled by just the right amount of human supervision. We spoke with Dr. Banga about continuous security posture assessments, contextualization, automated mitigation workflows, and what it means to calculate and reduce digital risk in a modern business environment.

TAG Cyber: *With all the tools and technologies we have today, why is quantifying the attack surface per company still so complicated from a technological point of view?*

BALBIX: Let's consider the size of attack surface of a typical enterprise. You might be trying to protect tens (maybe hundreds) of thousands of assets that belong to your organization. Each asset can be compromised in hundreds of ways.

To compute the breach risk of each asset, you need to consider 5 things: asset vulnerabilities, whether these vulnerabilities are being exploited in the wild, the level of exposure of the asset based on how it is used, the presence of any security controls, and the asset's business criticality.

Then there are at least 3 ways in which a compromised asset is impacted: confidentiality, availability, and integrity.

Multiplying these factors to get a back-of-envelope estimate: $15000 \times 400 \times 5 \times 3$ gives us 90 million factors that need to be continuously observed and incorporated into the enterprise risk calculation. This is not something you can do easily.

Since adversaries tend to target the weakest link, you do need to worry about the complete picture. Any factors you leave out in the calculation above mean you are blind and potentially exposed at the corresponding part of your attack surface.

Reality is even harsher. Most enterprises do not have an accurate picture of their asset inventory. They do not have a full picture of the different types of vulnerabilities and threats, nor do they know the efficacy of their security controls or which assets are most important.

Multiplying these factors to get a back-of-envelope estimate: 15000 x 400 x 5 x 3 gives us 90 million factors that need to be continuously observed and incorporated into the enterprise risk calculation.



TAG Cyber: Why isn't a holistic vulnerability management program, with vulnerability scanning, pen testing, business impact analysis, and incorporating CVEs, for instance, good enough?

BALBIX: Vulnerability assessment is a good start to understanding risk. However, traditional vulnerability management programs miss big chunks of asset inventory. They don't cover many non-CVE risk items such as password reuse, misconfigurations, user behavior, and more. Vulnerability tools also don't understand the compensating effect of deployed security controls. Simply mapping vulnerability metrics to business risk doesn't work because it's missing many factors.

There are many other problems with the way traditional vulnerability management programs are run. Often, there is only episodic assessment when periodic scans are run, which means the picture at any one time is probably a stale snapshot of the past. Organizations don't calculate their mean-time-to-patch (MTTP), which means they don't really know the fraction of time they spend exposed. Business impact analysis is often performed using subjective metrics such as "high," "medium," or "low" rather than in currency terms (e.g., Dollars, Euros, etc.).

Therefore, CISOs and security teams need to do a lot of manual work to gather information from multiple reports and different tools to calculate their overall cyber risk. Many organizations don't even try.

TAG Cyber: What are the questions your customers—CISOs, specifically—want answered about cyber risk posture?

BALBIX: CISOs have three requirements about cyber security posture:

1. The Big Picture: A unified, up-to-date, comprehensive view of their security posture with accurate risk calculations that incorporate cyber security context and business context.
2. An Operational View: Dashboards, planning tools, workflows, notifications, reports, and more that are integrated with various security and IT tools. The operational view of cyber risk posture helps security teams prioritize projects while enabling the maximum automation and gamification of risk mitigation activities.
3. A Board Level View: An executive view of the big picture, suitable for demonstrating the overall state of the cyber security program to senior executives and board members in business risk terms, while still being firmly tied to the actual on-network conditions.

TAG Cyber: How does Balbix BreachControl™ work?

BALBIX: In a nutshell, Balbix is about maximum automation of everything needed for cyber risk identification, prioritization, mitigation, and visibility.

Balbix starts by gathering all relevant cyber security and IT data from deployed IT and cyber security tools and directly from the network and endpoints. Note that this telemetry incorporates

data about servers, desktops/laptops, network equipment, smartphone/tablets, IoTs, applications, users; managed or unmanaged; on-prem, mobile, or cloud-based.

This data is constantly deduped, collated, and analyzed to implement automatic asset inventory, and continuously assessed for risk across all assets and 100s of attack vectors. No scans are needed. As new assets are deployed (or old ones repurposed or retired) and as new vulnerabilities become known, Balbix automatically identifies them and recalculates risk, accounting for security and business information. We use proprietary machine learning algorithms to make these complex tasks tractable.

After evaluation, prioritized sets of vulnerabilities are automatically dispatched to the risk owners for supervised and automatic mitigation. Balbix takes into account any exceptions that may have previously been specified. For example, you may have chosen to temporarily accept risk from a CVE because the asset is due to be retired soon. Balbix also lets CISOs specify and manage the risk ownership hierarchy in a systematic fashion. Risk owners have access to all the information, tools, and integrations for automatic as well as supervised risk mitigation.

The cycle is data-driven and highly visual. Each stakeholder has access to contextual dashboards that enable them to do their part in cyber risk reduction.

The role of AI is key in gathering and crunching data. What we do, essentially, is mimic the capabilities of your best cyber security and risk experts, at scale. Unlike human experts, AI models are very good at calculation in 100-dimensional space and can run 24x7 without tiring.

Another key capability we bring is gamification. Forward-leaning CISOs have been trying to do this for many years and Balbix provides a platform to publish risk leaderboards and owners.

TAG Cyber: How does Balbix manage the “invisible” threat?

BALBIX: By automating asset inventory, Balbix attempts to minimize one component of the “unknown” by accurately identifying things security teams are responsible for protecting.

A second factor of the “unknown” is adversary innovation. We address this by continuously updating models of attack vectors and sequences that we consider in our risk calculations.

The last factor of “unknown” is the human element—human actors will periodically make mistakes and behave in irrational, even malicious ways. This axiom is incorporated into our models and calculations.





AN INTERVIEW WITH ROGER KAY, VICE PRESIDENT OF SECURITY STRATEGY, INKY

IS YOUR EMAIL WHAT IT PURPORTS TO BE?

Phishing and email compromise have been around for as long as digital communications have existed. Early examples of phishing seem silly in hindsight, and modern attack tactics and techniques can be almost impossible to detect, especially when relying on busy humans' eyesight and Bayesian models as backups. However, phishing remains the number one attack vector; it persists because it works. As defenders grow smarter and technologies evolve, savvy cyber criminals evolve alongside those technologies, learning new tools' capabilities and creating craftier ways to work around them. Even with a plethora of current technological defense capabilities, phishing is a massive business risk.

INKY was founded in 2015 by Dave Baggett and Simon Smith to fight back against phishing, fraud, and email integrity attacks. Roger Kay, Vice President of Security Strategy at INKY, spoke with us about how phishing has evolved (i.e., why it's more than malicious attachments and infected links) and what they're seeing in an age when email use is higher than ever, thus giving attackers greater surface of opportunity.

TAG Cyber: *Tell us about INKY's history: Why was the company founded, what are your/the founders' backgrounds, and how does that play into what INKY offers today?*

INKY: I've known Dave Baggett since he was in grad school at MIT studying artificial intelligence. At the time, he was just a kid working for me in a small software company, International LISP Associates, that had one project with one customer: a multilingual text processor for the National Security Agency. He would do amazing things like write an entire compiler overnight. I knew I wanted to keep an eye on him.

From ILA, Dave went off and co-founded Naughty Dog, a videogame producer, making his first stake there. He rolled that into ITA Software, which optimized the airline database. Dave and his partners sold ITA to Google in 2010; it's what now runs Orbitz, Kayak, and other airline sites.

From that point, Dave just wanted "to fix email." Email was (and still is) a huge, broken system that loosely connects potentially 3.5 billion addresses around the world, and the experience is ugly.

Fixing email turned out to be too ambitious; so, after several pivots, the INKY team decided to take on phishing attacks (which were beginning to ramp up), reusing some of the learning from the end-to-end effort. The first version of that was also client-based, and for the same reason, failed to ignite. But the interest was there.

After a bit more discussion about where to place a cloud offering and how it would be designed, the team settled on an in-line virtual appliance that sits between the secure email gateway and the client device. Around that time, we raised funding, began to build staff, and acquire customers. Today, INKY Phish Fence has more than 500 customers.

A skilled phisher can take a real email that links to a real web page and change just a few invisible or nearly invisible things, and it looks just like a good one.



TAG Cyber: Most people think of phishing as a basic problem that's hard to solve. How is INKY's approach different than that of traditional anti-phishing or SEG providers?

INKY: First, let's distinguish between spam and phish. Spam is high volume, low threat. Phish is low volume, high threat. A SEG, or even Microsoft, uses a reference pool of characteristics of good and bad emails and applies that to each new candidate. If an email looks like one the provider recognizes, then they tag it "good" or "bad." The problem with this type of analysis is that a well-crafted phish looks like a good email. A skilled phisher can take a real email that links to a real web page and change just a few invisible or nearly invisible things, and it looks just like a good one. There's only one poisoned link. The SEGs will let it through, and it has a payload that will tie up the whole network in ransomware, eventually fool the assistant comptroller into sending \$75,000 to that bank in the Cayman Islands, cause the company's valuable proprietary IP to migrate to China, lead to the CEO's resignation due to the publication of his private correspondence, or grind the company's operations to a complete halt.

INKY analyzes an email on first principles; it derives its judgment about an email from things in the email itself rather than from a pool of known threats. INKY looks at an email two ways: like a person and like a machine. The person side uses computer vision to "see" what the email is trying to be (e.g., a notice "from" Microsoft or Citibank). The machine side checks where it's really from. If the two don't line up, INKY flags the email.

INKY-as-a-service is a few different modules which analyze an email in fewer than two seconds. Each module derives its own conclusion and confidence level and sends that information as a "vote" to the aggregator. That aggregated value is what INKY uses to decide how to tag the email using a color-coded banner to alert customers to the suspicion level: gray for neutral, yellow for caution, and red for dangerous. In addition, each module that hits its own trigger value inserts a text warning into the banner. So, the recipient sees all the reasons INKY didn't like the mail. The banner also has a "Report This Email" link that allows recipients to give feedback that gets incorporated into the model.

Another differentiator is that INKY doesn't rely entirely on regex, regular expression pattern matching. Regex can be fooled by a string like "563 eciff0," which, when embedded in the email's HTML, looks like a random string to the analyzer running through it. Instead, INKY renders the email for visual analysis, correctly identifying the email and removing the threat.

TAG Cyber: What are some recent attack trends enterprise need to be aware of?

INKY: Attack trends migrate with the news cycle. Today, getting ready to go back to offices after COVID is a rising meme. Government notices, HR policy updates, insurance pitches, medical information—all these give phishers plausible cover. They ask what you are most afraid of and that's the anxiety at which the phishers aim. On a broader scale, payloads are getting more complex. The phishing email is just the impetus to start a whole conflagration. For example, the immediate intent may be credential harvesting, but those credentials will be used for other purposes: to move laterally through the organization, to steal money or secrets, to rally botnets, to deliver a sudden and comprehensive ransomware shutdown. In recent times, we've been seeing more emails that strive for VIP impersonation, but have no links or attachments, just an instruction from your CEO to do something on the QT.

TAG Cyber: Isn't phishing/social engineering a never-ending battle? As soon as detection capabilities evolve, won't the attackers just evolve to evade detection?

INKY: Yes, that's true. We are always incorporating new things into our models and refining existing models. But we're not in the whack-a-mole business. We're not building an endless database of known bad patterns. We're only asking, "Is this what it purports to be?" A better evolved scam to more realistically impersonate Microsoft will still fail if INKY determines that the email came from a stolen account in machine shop in Jakarta. The machine shop may be real, and it has every right to send email from that range of IP addresses, just not email on behalf of Microsoft.





AN INTERVIEW WITH AARON TURNER,
FOUNDER AND CEO, SIRIUX

HOW SECURE IS YOUR MICROSOFT SAAS DEPLOYMENT? DO YOU KNOW?

Microsoft provides the prevailing business productivity suite across the world. Microsoft 365 (formerly Office 365) includes more than 30 different applications to help workers communicate, collaborate, and create.

With such deep business roots, the security of the suite, its applications, and its configurations are a concern for companies wanting to maintain the confidentiality and integrity of the work done on their behalf in M365. Considering Microsoft is also a leading cyber security provider, businesses would be wise to think that M365 has extensive security baked in. And it does. Except it's nuanced.

Aaron Turner, CEO at Siriux, has his own long history with Microsoft. Turner's latest venture is helping businesses understand their security posture and exposure from M365. We spoke with Turner about why companies need to pay more attention to what they don't see in the suite.

TAG Cyber: *You've worked for, built, and sold many successful security companies over the years. How did you come up with your newest idea, and what problem does Siriux solve?*

SIRIUX: A few years ago, I was advising a large insurance company on how best to apply security governance and policy for a migration of 50,000 users to Microsoft 365 within a few weeks. Microsoft's documentation was lacking, and the staff didn't know what had been configured. I realized the source of truth was in the software itself, but I didn't have access to it. If I could have queried the security settings automatically, I could have efficiently identified their true M365 security configuration.

Then, while on mandatory lockdown last spring in Luxembourg during the pandemic, I decided to put my research to use and start Siriux. A few months later, after getting permission to relocate my family back to the U.S., I found great technical folks to help polish my ideas and get the Siriux scanning platform ready for testing.

Last fall, the M365 ecosystem suffered tremendous security disruptions and Siriux was in the right place at the right time. We were invited to help several Dark Halo victims remediate the vulnerabilities in their tenants and harden them against future attacks. We learned how sophisticated adversaries exploited the complexity of M365's configuration options and started to hunt for those adversaries through our scanning tools.

TAG Cyber: *Why are these settings not more transparent or easy to manage?*

SIRIUX: Ease of use often conflicts with security! To be fair, Microsoft has built a complex

Most of the high-criticality security settings are only available through either the M365 PowerShell modules or the Graph API.

collaboration platform designed for worker productivity and collaboration. In its default state, it is ideal for marketing folks or other business units who don't have an inherent need to keep information secret. However, most organizations need more customization to effectively

protect the identities and data stored in M365's applications. Some security settings are harder to discover in M365 due to interface limitations more than anything. Most of the high-criticality security settings are only available through either the M365 PowerShell modules or the Graph API. Those don't have user-friendly interfaces so security personnel must discover and configure them through command-line tools.

TAG Cyber: In your experience, are enterprises, even ones with large security teams, aware of the scope of the problem?

SIRIUX: Microsoft has done an excellent job of building trust with customers. Their Security and Compliance Center provides an excellent starting point to improve security. However, they struggle to educate security teams about the true risks. For example, most IT operations teams synchronize the on-premises Active Directory without fully understanding its potential vulnerabilities. Most organizations we work with don't restrict which M365 services and applications users can consume. Do they know what Kaizala, Sway, Delve, Power Automate, and others mean to overall cyber risk posture? Maybe not. Siriux helps expose these risks.

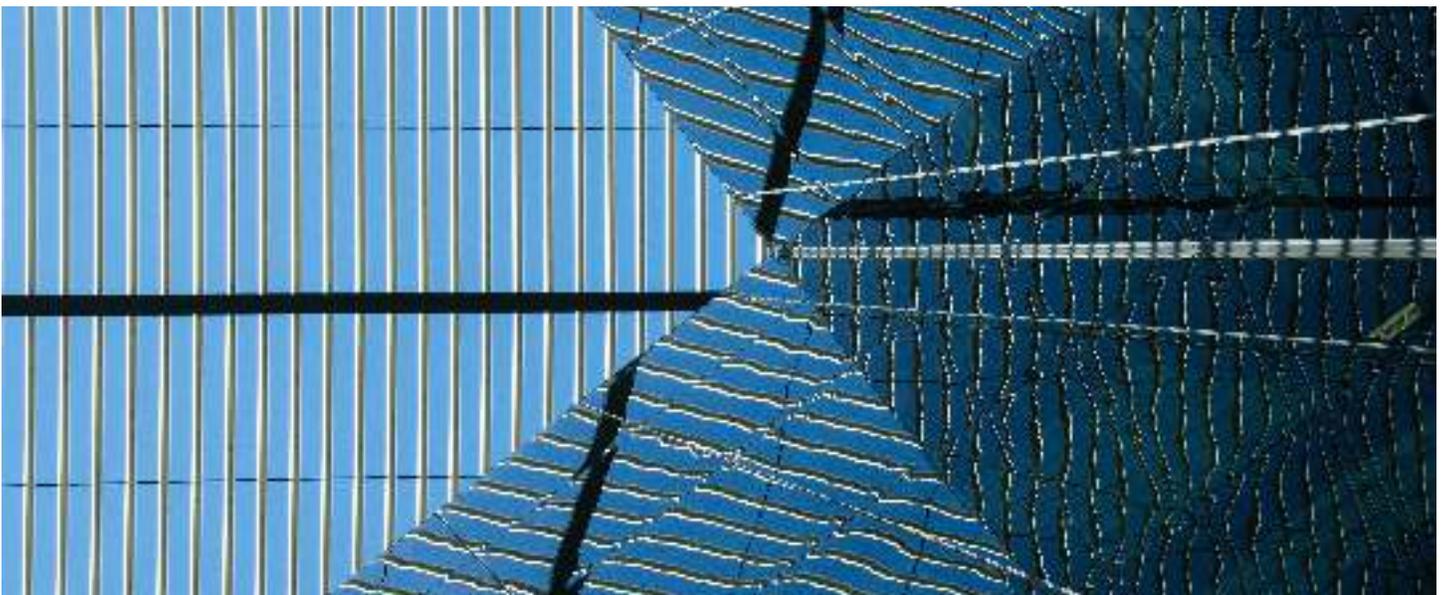
TAG Cyber: The media love to make a big deal when Microsoft is compromised, but the reality is that they're a big target, a big prize. Does this cause a trickle-down effect for businesses and how they approach security of their Microsoft deployments?

SIRIUX: Microsoft has always had a huge security target on its back because of market share; attackers go where the victims are. I get a bit defensive when Microsoft is criticized too harshly because I participated in security improvement projects there in the late 90s and early 2000s. Plus, Microsoft has shown the industry how to respond to a global-scale security incident more recently. Their transparency has helped businesses better understand the risks associated with using their technology. Just like Microsoft customers suffer en masse, they also enjoy the benefits of Microsoft's security investments, which will bear fruit for years to come.

TAG Cyber: The Microsoft Exchange breach in March was a wake-up call to companies with on-prem deployments. But the cloud brings different challenges. Aside from using Siriux, what are the top strategies for protecting cloud deployments?

SIRIUX: We get this question a lot. Here's what I recommend:

- Follow the NSA's guidance: If you're an M365 customer, eliminate third-party identity providers; they don't offer much value for protecting M365. Yes, this can break SSO deployments, but the potential for badness in the identity provider trust chain is just too great until we see further innovation.
- Eliminate the use of authenticator apps by privileged users. SMS one-time codes, mobile app code generators, and push authenticators are all major attack targets. Smartphone-dependent technologies are just one iOS or Android vulnerability away from being cloned. The iOS vulnerabilities fixed in a recent iOS security update were directly related to authenticator compromises observed among global M365 enterprise users.
- Disable any unapproved M365 service to block users from accessing them. Just like any attack surface reduction process, enabling fewer applications will result in near- and long-term security benefits.
- Endpoint security matters now more than ever. A strong focus on endpoint hygiene (security update installation as well as EDR) will help in the battle against attackers who are trying to pivot into M365 tenants to persist and exfiltrate data undetected.





AN INTERVIEW WITH OM MOOLCHANDANI,
CTO, CISO, AND CO-FOUNDER, ACCURICS

PREVENT BAD CODE COMMITS FROM CAUSING A MEGABREACH

DevOps is one of the most business-altering processes of the last decade. The pace at which companies can plan, build, and deploy software requires an entirely new strategy. As is no surprise to anyone reading this Quarterly, DevOps has also impacted how we must think about the software development lifecycle (SDLC).

Reality is, security has been less successful at integrating into DevOps than we'd hoped...and tried. First-generation tools continued the trend of bolting security on to later stages in the development process and used network "speak" to protect applications, which was ineffective. More recently, a crop of ex-developers has gotten their hands around the problem by building more dev-friendly, cloud-native tools.

Accurics is one such company aiming to fix a broken process by focusing their platform on infrastructure as code (IaC) and helping companies detect and remediate policy violations and breach paths before cloud infrastructure is provisioned. We spoke with Om Moolchandani, CTO, CISO, and Co-Founder at Accurics, about their platform and philosophy.

TAG Cyber: *What is the true scope of cloud-based, application-focused breaches?*

ACCURICS: Today, cloud computing touches nearly every aspect of modern life, and it's safe to say that every company is a software company, likely relying on the cloud more than ever. It's natural that cloud breaches are increasing in scope and scale—in the last three years alone we've seen more than 30 billion records exposed in the cloud.

There are a few trends contributing to this growth, including increased adoption of managed services and the use of Infrastructure as Code (IaC). Cloud automation is critical to maintaining development velocity and scale, but it also creates fundamental risks to the integrity of the delivery process.

As we saw with the SolarWinds Orion attack, adversaries are striving to exploit weaknesses in these assets in order to deliver malware to end users, gain access to production environments or data, or completely compromise a target environment. Previously, managed services were hidden within an organization; now they're largely exposed to the world. When misconfigurations are exploited in development pipelines, for example, it can be truly disastrous for a company and its customers.

TAG Cyber: *What, exactly, is the DevOps shift to IaC and how does that impact security?*

ACCURICS: These days, developers are writing application code, IaC, and many are beginning to adopt GitOps, which is using technologies like Helm and Kustomize to codify deployment processes—something previously done through

Of all of the violations identified in our research, 22.5% correspond to poorly configured managed services offerings.



the operations team. These practices give development a lot of flexibility, and automation helps them deliver software more quickly. But we're giving up opportunities for manual sanity checks in the development and deployment processes. All it takes is one bad code commit to create a breach path for hackers to exploit, so security needs to be approached differently.

The challenge is that existing security tools were designed to be used during deployment or in runtime by security pros. That doesn't work for DevOps. Security in runtime is too late because vulnerabilities are already exposed to attackers. Deployment is automated, so security now needs to be integrated into automated processes, and the tools can't presume security expertise because developers are generally not security experts. You need tools that are effective and that don't get in the way, and you have to find a way to ensure that developers are able to easily understand security findings so they can be fixed.

TAG Cyber: What are the benefits of remediating in IaC versus during runtime?

ACCURICS: First of all, IaC exists before the runtime is provisioned. By finding misconfigurations early, in IaC, we have a chance to fix them before they can be deployed to runtime and exploited. It can also be easier because IaC developers have the context they need to understand why things are configured the way they are, and they can fix the problem without breaking something else. One area where organizations often struggle is remediating in IaC, after a problem is detected in runtime. Most fixes are applied in runtime, because we obviously want to stop the bleeding as quickly as possible. But when a misconfiguration is remediated in runtime, that fix is only rarely pushed back to the IaC.

Why is this important? The next deployment is going to reintroduce the problem that was just fixed. You can find and fix it in the runtime again, but (a) that's a waste of resources, (b) it's exploitable until it gets fixed, (c) it is often harder to fix things in runtime without breaking something else, and (d) the list of things that need to be re-fixed will grow over time and become an unmanageable burden of security debt. Tools that fix problems in IaC, regardless of whether they were found in IaC or runtime, avoid these problems. You fix it once, it stays fixed, and you don't need to think about it again.

TAG Cyber: Your message is that Accurics programmatically detects and fixes cloud infrastructure misconfigurations in design, build, and runtime. Briefly, how is this accomplished?

ACCURICS: The Accurics Platform provides developers with a path to create secure code from the start—without asking them to be security experts. It contextualizes issues through automated



threat modeling to programmatically detect breach paths using both IaC and runtime configurations. It breaks kill chains by generating the IaC code required to eliminate the breach path and delivering fully baked fixes to developers. The developer simply needs to review the code that we've pushed to them, approve it, and merge it into their codebase. It

provides full-lifecycle security, addressing best practices, compliance, drift, and security use cases, and it enables teams to establish and maintain a secure posture with minimal effort.

TAG Cyber: You recently published your Cloud Cyber Resilience Report. What are some of the more interesting or surprising findings?

ACCURICS: Earlier we spoke about the increased adoption of managed services like FaaS—that adoption is actually happening at an extraordinary rate. We were surprised to find that, of all of the violations identified in our research, 22.5% correspond to poorly configured managed services offerings. The vast majority of these violations are due to the use of default security profiles or configurations that provide excessive permissions. We see time and again that developers expect default configurations to be fit for purpose, but they seem to forget that the CSPs providing these services have different goals than the developers that use the services. Default configurations for managed services are often designed to make it easier for developers to get started with a service—which means that they favor more permissive rather than more restrictive access. By using defaults in normal use, organizations are making it easier for attackers to discover their services, read their data, and potentially modify things.

The surprising thing is that organizations have been struggling with these same dynamics with storage buckets and object storage for years, and it's still a big problem. I worry that as adoption of managed services takes off, we're going to see an explosion of breaches attributable to these insecure configurations. In the cloud-native community, we really need to get our arms around this problem and make it harder for developers to make these mistakes.



AN INTERVIEW WITH YOSSI APPLEBOUM, CEO AND CO-FOUNDER, SEPIO SYSTEMS

HOW TO GAIN CONTROL OF THE HARDWARE SUPPLY CHAIN

“Software is eating the world,” words infamously spoken by Marc Andreessen, may connote that software is the critical element in a cyber protection strategy. Coupled with organizations’ intense focus on application development and use, it’s easy to see why many vendors place efforts in securing software.

But overlooking hardware assets is a grave mistake. IT, OT, and IoT hardware devices are the endpoints which can be—and are—exploited by threat actors. These initial infiltration points can lead to larger compromise. What’s more, today, networks must be able to accommodate myriad device types without adding risk. This requires a thorough understanding of every device touching the network, establishing baselines, and understanding which assets have—and should have—access to what other resources.

Sepio Systems helps companies gain control of hardware assets and manage hardware access controls to prevent compromise and policy violations. Yossi Appleboum, CEO and Co-Founder at Sepio, recently spoke with the TAG Cyber analysts about the problem and Sepio’s solution.

TAG Cyber: *What are some of the hardware threats and exploits that have popped up lately that people might not be aware of—but should be?*

SEPIO: The new normal, work from home, hybrid work, and other names that describe how our work environment changed due to the pandemic altered the way organizations secure themselves, but it also changed the way threat actors work.

In the last year, we have seen a spike in the number of hardware-based attacks on remote workers and on empty corporate buildings, ranging from supply chain manipulators altering corporate devices on their way to home offices, and insiders implanting hardware attack tools in corporate backbone networks and data centers. The number of uncontrolled peripheral devices connected to corporate issued laptops jumped by x10. The number of private computers connected to corporate networks jumped by x5. The number of Wi-Fi based attacks on remote workers using their corporate-issued access points or their existing Wi-Fi equipment jumped by x25.

TAG Cyber: *What kind of data and insight do customers get from your solution?*

SEPIO: Our Hardware Access Control solution, HAC-1, provides full visibility of all hardware assets, from PC peripheral devices to connected IT/OT/IOT devices. Our visibility enables organizations to manage and prioritize the risk from hardware devices by providing a risk score and risk description per each hardware element. We provide visibility to see all devices including unmanaged, MAC-less, spoofed, and transparent devices. Sepio’s HAC-1 augments physical layer

The number of Wi-Fi based attacks on remote workers using their corporate-issued access points or their existing Wi-Fi equipment jumped by x25.



(Layer 1 fingerprinting) and other sources of data in combination with big data and machine learning to discover unknown attack tools and vulnerable devices without the need to configure any permit-/blocklist and without the need to set any baselines.

TAG Cyber: How are companies using the data they get from your platform?

Sepio: Many of our customers are feeding other cyber systems with our data for creating a better solution for network access control (by integrating HAC-1 with a NAC), completing zero trust frameworks (by feeding micro-segmentation solutions with our data), increasing asset and risk visibility (by feeding systems as CMDB, SIEM, and EDR), and handling incident management (by integrating with SOAR tools). Sepio's HAC-1 can be used as a standalone solution for generating and viewing reports, tracking events, creating policies, and threat hunting, but we believe that a significant part of our value is by feeding other security systems totally blinded to the hardware risk with our actionable data for a better security posture.

TAG Cyber: Isn't risk incredibly personal to each organization depending on their risk tolerance, deployed assets, compliance mandates, and more?

SEPIO: Yes, it is totally personal. But we are taking organizations from an uncontrolled/unknown risk situation to being able to control and manage it through custom settings. For instance, we have customers that prioritize business continuity over security, so they raise the risk threshold higher. Some of our customers do not allow any private devices to be connected to their corporate network while others restrict only media devices and so on. It's very personal.

There are 100s of different use cases based on verticals, geography, regulation, compliance, and more.

TAG Cyber: The government has increased its requirements on hardware. Can you tell us what that looks like and why private enterprises should take note?

SEPIO: In the last few years, we've seen the government starting to take public action against adversaries. For many years, it was difficult to find any public comment from government officials about the risk stemming from hardware devices. Recently, we hear government officials, including the president himself, briefing the public about the risk coming from our supply chains and discovered cyber activity of foreign nations.

We are also starting to see legislation and regulation around cyber. A great example of that is [Section 889 of the NDAA](#), which lists several vendor products that are forbidden to connect to federal infrastructure. This is a very important step in securing our

critical infrastructure, but it is only one step in a very long road that will bring us to better control of supply chains and set a cost for bad actors who get caught.

Using hardware devices as attack tools is not limited to governments; we see an increase in threat actors using hardware devices to attack private enterprises all around the world. Financial institutions, healthcare, pharma, manufacturing, and critical infrastructure are all suffering from hardware-based attacks and, in many cases, without seeing it running for a very long time. Private enterprises must gain control of their infrastructure, manage all connected devices, learn the associated risks, and then start prioritizing the mitigation of these risks.

We all witnessed the results of a penetrated software supply chain during the SolarWinds incident. Let us all now ask a simple question: How would our morning look after discovering a massive hardware-based incident? I strongly suggest that we be ready for that. There is no “if,” but only “when.”





AN INTERVIEW WITH TIM WAINWRIGHT,
CEO, SRA

AMP UP YOUR SECURITY PROGRAM WITH YOUR SECURITY CONSULTING PARTNER

Over the years, cyber security services have played an important role in cyber security. First, as cyber security became a field adjacent to but distinct from IT, and now as the industry faces a talent supply shortage, independent experts have stepped up to offer an economy of scale that many organizations are unable to support.

The most successful security consulting firms attract experts who want the challenge of applying their specialization across diverse companies using the skills they've acquired while gaining a broad understanding of adversary tactics, techniques, and procedures (TTPs). Security Risk Advisors (SRA), an 11-year-old consulting firm based out of Philadelphia, has been the go-to for major enterprises and non-profits alike, helping them with security testing, simulation, and cloud security services, as well as a variety of other must-have capabilities for the modern organization. TAG Cyber spoke with Tim Wainwright, CEO at SRA about how their role as advisors and consultants has changed as the industry has evolved.

TAG Cyber: *SRA was founded in 2010. What major changes have you observed across your customer base over the last decade?*

SRA: We started SRA before almost all the major data breaches, a time when cyber security was nowhere near the priority it has become for the board—and even internal organizations, themselves—today. Ransomware, third party risk, the need for effective detection controls, and NIST CSF and MITRE ATT&CK alignment have become priorities for all types of organizations—even healthcare, which was reluctant 10 years ago but which is now our third largest client vertical.

TAG Cyber: *Anyone could, theoretically, use their experience in security to become a “consultant,” but that doesn’t necessarily mean they’ll be successful. What does it take to be an effective security consultant in 2021?*

SRA: Consultants need to do three things very well. 1) Continually develop knowledge that outpaces what clients can do for themselves, 2) Help clients translate, communicate, and operationalize that knowledge into effective, measurable controls, and 3) Challenge the status quo.

On this last point, there are some answers to security problems that have become very comfortable for boards and audit committees because of their simplicity and familiarity. Consultants today need to challenge and develop effective new approaches to old solutions like pen testing, third-party risk, password policy, and identity and access. There is a place for all these, but their assumed priority

Security teams don't have a good way to document, repeat, and report on their work—it's another complicated effort that surpasses Microsoft Excel's usefulness.



and legacy approach underperform and consume a lot of resources.

TAG Cyber: SRA focused for many years on traditional services like testing, strategy, and CyberSOC services but you now offer "Purple Teams." What is it?

SRA: My definition of Purple Teams (sometimes "attack simulations") is an open-book-exam process that prioritizes and demonstrates quantifiable improvements in defenses over time. All our clients have GRC teams, smart security engineers, and some of them have invested in their own red team capabilities. Purple Teams is the ultimate process to set the direction and coordinate their work together. The scope of testing techniques is more comprehensive than either pen testing or red teams and it gives credit for controls that work well as much as it identifies gaps. The specific gaps in detection give security engineers confirmed and agreed priorities. The Defense Success Metrics from Purple Teams lets GRC validate, report, and track simple, meaningful metrics. The most important aspect of Purple Teams is the teamwork and knowledge sharing. We love to facilitate this process and teach our clients how to do it. As we say at SRA, everyone "Levels Up."

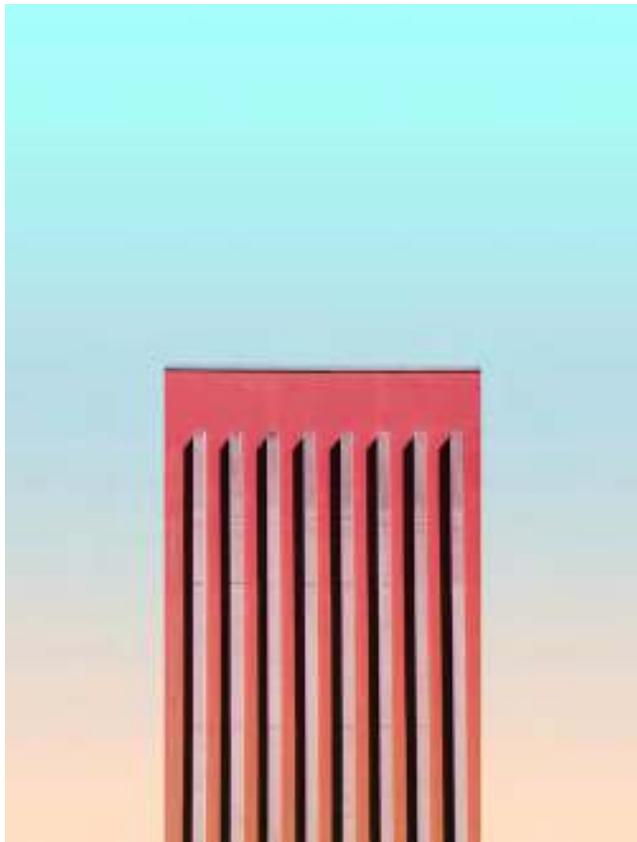
TAG Cyber: Why was it important to develop this service now?

SRA: Our clients want to take a threat-driven approach to their security program. This means that they want to refocus on defending against threat actors instead of just pleasing auditors and compliance mandates. I wish there were a stronger intersection but unfortunately that is not the case. Purple Teams aims to simulate threat actor tactics and confirm controls will block or detect as expected. Purple Teams uses MITRE ATT&CK to form the scope and basis of Defense Success Metrics. The reason why this service is needed now is because security teams don't have a good way to document, repeat, and report on their work—it's another complicated effort that surpasses Microsoft Excel's usefulness.

So, for this reason SRA developed and maintains VECTR (vectr.io), a free tool for the industry that is being adopted quickly. We use it in our engagements but had the vision that it could be an excellent freeware platform—which to us means too good to be free. At least three SANS classes teach students how to use it, and we see more and more conference presentations all over the world reference VECTR. In a way, SRA wrote the book for modern purple teaming and it's done a world of good for organizations who want to measure their posture against threat actors and their techniques.

TAG Cyber: When a company is hiring a security consultant, what are some things they should ask themselves and the prospective firm to ensure a successful engagement?

SRA: Some of the key questions are: Is this company on the bleeding edge but able to adapt their approach and recommendations to our size, resources, and business needs? What contributions do they make to the industry, outside of paid engagements? Are they going to be independent when it comes to recommendations or do they also sell solutions (i.e., are they going to be constantly trying to upsell me)? Are they more focused on my organization's success or their own growth?





AN INTERVIEW WITH NONG LI, CO-FOUNDER AND CTO, OKERA

DATA AUTHORIZATION WITH PRIVACY BY DESIGN

Data lies at the heart of every business. From financial data to customer data, product data, to business strategy and operational data, there is clear a reason data has been dubbed the “crown jewels.” However, businesses amass so much data, and in so many places, that it is extremely difficult for most security teams to get their hands around the scope of what they need to protect, much less affect a governance and protection strategy that covers all data types and locations. This is especially true given the number of employees, contractors, partners, and systems which all require data access—without raising enterprise risk.

Okera is a universal data authorization company that complements data governance to fulfill any data access use case. The company is based in San Francisco and helps businesses create and manage fine-grained data access policies for data in their data lakes, data warehouses, and cloud instances. Nong Li, co-founder and CTO at Okera, recently spoke with the TAG Cyber analyst team about secure data access and authorization and explained why Okera provides the “missing piece.”

TAG Cyber: What are the current challenges organizations face when it comes to secure and compliant data access?

Okera: As organizations navigate through growing oceans of data to source digital transformation efforts, they are also battling role explosion and controlling who should have access to what data and when. Adding more complexity is the increase and evolution of data privacy regulations such as GDPR, CCPA/CCRA, etc.

Organizations need to balance providing data agility while protecting the business, customers, and partners from unauthorized or unnecessary access to sensitive data and PII/PHI, which can lead to risky misuse, data leaks, and breach exposure.

Existing technologies cannot manage the complexities created by the trifecta of expanding data lakes, data consumer roles, and privacy regulations because they apply to a narrow, specific set of use cases. The access primitives are incomplete or not right for data. Organizations need a new framework that provides efficient access to the right data at the right time, with fine-grained access control to the individual table, column, row, and cell level based on roles, geography, and data attributes.

There is also extreme complexity in policy management. The more data sets, regulations, roles, and applications added means policy management becomes exponentially more complex and untenable to govern. Organizations need to rethink how to approach this problem.

Lastly, audit and alerting systems do not

Data authorization is the discipline of making sure every data request is business-purpose appropriate, enables digital transformation, and includes data security and privacy by design.



understand data access patterns and can't make unauthorized access to data actionable. Audits are at an infrastructure level and do not capture semantic information needed for real visibility into what sensitive data are potentially at risk.

TAG Cyber: Why focus on data authorization and access?

Okera: Things go bad when people—and now systems and algorithms—have access to data they shouldn't, or they cannot get access to the data they need for legitimate business purposes. Data authorization is the discipline of making sure every data request is business-purpose appropriate, enables digital transformation, and includes data security and privacy by design.

Providing role-based, attribute-based, and policy-based access controls (or what we call fine-grained access control) to data for internal and external partners alike with speed and agility to meet business needs while ensuring data does not get leaked, breached, or misused is critical. Having a granular, data-level auditing system to gain visibility into who is accessing what data and when, and which access policies were implemented, enables security leaders to act and remediate against risky or unauthorized data access.

By instituting a framework built for secure data access and authorization, organizations can provision data faster to accelerate business agility, reduce the overall attack surface, minimize data security risk while complying with data privacy regulations, and provide visibility, auditing, and reporting into who is accessing data when, while reducing overprovisioning of applications.

TAG Cyber: Isn't it hard to manage access requirements given the continuously changing needs and always-expanding data sets, role explosion, and evolving regulations of most businesses?

Okera: Without a modern approach to universal data authorization, I'd say it's impossible in our post-big data, post-GDPR era. The phrase "right data to the right person at the right time" has been banging around for years now. The pipedream (at least from the vendor's perspective) used to be that enterprise software would swoop in and you'd standardize everything on one platform and all would be well. But the truth is that enterprises are organic. The amount of technology diversity in established companies is astounding. You need to think about data authorization holistically.

Additionally, most organizations do not have appropriate attributes set on users within their identity access management (IAM) and LDAP systems.

That's where Okera comes in. We sit to the side, where you

manage data access controls as policies, and data requests are authorized like the transactions they are. Okera provides role-based, attribute-based and policy-based access controls—down to the cell level—in an elegant and efficient way. As a universal data authorization framework, Okera provides a critically important and highly performant way for organizations to protect their data, customers, and partners.

In addition to the Okera Dynamic Access Platform flagship product, Okera integrates seamlessly into existing data governance ecosystems with REST APIs. This makes it easy for organizations to ensure compliance and data protection with evolving data privacy requirements and regulations, regardless of their data deployment strategies. Okera can be integrated into SIEMs and cyber/fraud fusion centers.

TAG Cyber: What types of data does Okera help protect?

Okera: We protect data at the point where someone wants to query or process it. This generally means structured data that is stored in a data lake, data warehouse, lake house, or traditional relational database. Think anything from financial transactions to clinical drug trial test data to patient health records. It's almost any data-enabled use case spanning data science, business intelligence, even operational applications. If someone needs to access data, Okera can authorize exactly what you can see based on the nature of the query, the data attributes, and your profile.

TAG Cyber: How does your platform ensure compliance with the numerous data protection and privacy laws and regulation?

Okera: Great question. I'll summarize it as three critical capabilities: a universal policy builder that packages data access controls into general compliance policies, dynamic policy enforcement for all data access requests, and centralized auditing and reporting. There's simply no way to ensure compliance without full visibility into the who-what-when-where of data access. If you don't know what's happening you don't even know if you're compliant, right? Which means you can't course correct. When every client simply reaches out for a quick data authorization, you get that full visibility into exactly what's actually going on in real life—not just what the policy says on paper.

Finally, universal data authorization needs to work for everyone, including enabling platform owners and data stewards, to get the metadata they need and distribute data safely to the right data consumers. You need the right building blocks and security primitives that map to regulatory and legal requirements. CISOs and information security leaders need policies and audits. Finally, organizations need to unlock and drive business value so that everyone can use their data responsibly.



AN INTERVIEW WITH ORI EISEN,
FOUNDER AND CEO, TRUSONA

USING PASSWORDLESS AUTHENTICATION TO ELIMINATE ATTACK VECTORS AND PROVIDE SECURE ACCESS

Cyber security professionals have been declaring that “passwords are dead” for many years. The only problem has been that businesses won’t give them up! They’re known, pervasive, and relatively easy to use. However, after years of education and demonstration—including the considerable breaches that have occurred because of weak, stolen, or reused passwords—security teams have finally been able to convince business leaders to move away from password-based authentication to passwordless methods.

The shift to password reduction and/or removal is underway at enterprises worldwide. The aim is to improve digital assurance and lessen identity risk in the workforce. Trusona has been leading the charge in the passwordless revolution by offering a dynamic passwordless multi-factor authentication solution.

Recently we spoke to Ori Eisen, founder and CEO at Trusona, about how the company is helping enterprises mitigate the risk from common threat vectors such as phishing, password reuse, and credential stuffing.

TAG Cyber: *Aside from familiarity, why have businesses wanted to hold on to password-based login for so long?*

Trusona: As with every new technology, there is always an instinctual resistance to change. With passwordless solutions, I think there is distrust in how deceptively simple it appears to be—and that carries a misperception of not being secure. Additionally, there seems to be much confusion around what being “passwordless” is or isn’t because of the variety of different definitions touted by various vendors throughout the cyber security industry.

Once an organization overcomes the potential distrust and has a clear line of sight into why removing password-based logins is so important, there’s another mental barrier: the ease and viability of an enterprise-wide implementation. Businesses have dozens or even hundreds of enterprise applications of all different types—cloud-based, homegrown, legacy, or custom—and they aren’t sure where to even start. We have to understand their issues holistically and provide them with a path to passwordless authentication that is safe and certain.

TAG Cyber: *Doesn’t passwordless just give actors different attack vectors, not eliminate them?*

Trusona: While no security measure is completely foolproof, the perpetual onslaught of breaches since the invention of passwords in 1964 has clearly demonstrated their inability to offer meaningful protection, especially in modern times. Cyber

The perpetual onslaught of breaches since the invention of passwords in 1964 has clearly demonstrated their inability to offer meaningful protection

criminals have had decades to utilize increasingly sophisticated, innovative methods to poke holes in password-based security with perpetually advancing technology. There's a reason compromised credentials represent the largest threat vector.

As cyber threats continue to evolve, so must enterprise security. For example, modern approaches to authentication take advantage of cryptography, public key infrastructure (PKI), secure enclaves, biometric sensors, and leverage the smartphones we all carry to remove the core threats from credential-based attacks. With such measures in place—and without bad actors being able to reuse the same credentials across corporate and personal applications—new threats become much less scalable. A rapidly growing remote workforce has only deepened the need for greater protection, as various reports depict surging attack volumes in the last 12 months. Minimizing attack vectors and providing secure access anytime, anywhere has never been more critical.

TAG Cyber: The security industry has been adopting traditional 2FA/MFA as means of improving security, but it hasn't been effective enough. Why not?

Trusona: While attempts to strengthen credentials by adopting 2FA or MFA—often utilizing SMS, one-time passcodes, and hardware tokens—can add some levels of security, those additional measures still only cloak the decayed foundation of usernames and passwords. Similarly, password vaults can offer the same false sense of security, protecting databases that store passwords with the very same root issue: passwords. With that inherent vulnerability, hackers continue to find creative ways around the outer layers, leaving companies open to phishing attacks, keylogging, SIM swapping, credential stuffing, and more. To truly and significantly reduce the overall attack surface and virtually eliminate the risk of compromised credentials, we must remove passwords at the foundational level.

TAG Cyber: Aside from the obvious benefit of increased security, what are other demonstrable improvements of passwordless adoption?

Trusona: Removing usernames and passwords from the equation means not having to remember or type anything, inherently enhancing the user experience for employees and customers alike. Employees enjoy more productivity and less time spent jumping through ineffective authentication hoops, calling the IT help desk for password resets and trying to adhere to tedious password policies. Customers are more satisfied with a brand's experience, increasing usage, retention, and app adoption where applicable. Passwordless methods also help organizations meet

modern, stringent regulatory compliance, such as eKYC, AML, PSD2, and more without burdening customers.

At the end of the day, security is a business expense. Data breaches are very costly—at over an average of \$8 million per instance—and removing the most common attack vectors based on credential usage protects those dollars. Additionally, you can realize sizable cost savings by significantly reducing support calls due to password resets and account lockouts as well as preventing the loss of customers due to user frustration.

TAG Cyber: What is Trusona's Anti-Replay technology and how does it work?

Trusona: Trusona's patented Anti-Replay technology is a security measure that prevents session replay attacks. It's analogous to taking a snapshot of a perpetually flowing river at a moment in time—there will never be another snapshot that will be identical to this one where the water moves, splashes, and dances off the banks in exactly the same way. Similarly, at the time of an authentication, a unique data set is captured—including when and where the user tapped on the screen, the device ID, as well as other device-specific meta data. This data is compared with previous authentication data, and if the same set of data is seen, Trusona can be sure an attacker is attempting to replay a previous authentication event and the request is denied.





AN INTERVIEW WITH JOHN LOUCAIDES, VP FEDERAL TECHNOLOGY, ECLYPSIUM

ELIMINATE EASY TARGETS IN YOUR FIRMWARE

With today's distributed workforce, device security must be a priority concern for enterprises. While software vulnerabilities and the CI/CD pipeline get a lot of attention, all software, applications, and servers are accessed by devices—there is always an endpoint. And if the device, itself, is insecure, regardless of the security state of the software, cyber risk is introduced.

Making matters worse, devices—laptops, servers, routers—are comprised of dozens of hardware components, some of which may not be built with security baked in, from multiple places along the supply chain. Further, firmware running on devices is made up of millions of lines of code, much of which may not have been analyzed for vulnerabilities or patched when a vulnerability is discovered.

Eclipsium provides device security down to the hardware and firmware levels. We spoke with John Loucaides, VP Federal Technology at Eclipsium, about the company's platform and how it finds and fixes weaknesses and threats below the operating system, which, if left unchecked, subject companies to device tampering, ransomware, and breaches.

TAG Cyber: Microsoft recently published a report claiming that 83% of businesses have experienced at least one firmware attack in the past two years. Why do you think attackers are turning to firmware now?

Eclipsium: Over the past decade we have experienced significant enhancements to the security of operating systems, applications, and networks. These changes make exploitation much more difficult and lead to lengthy exploit chains and operational complexity for attackers. In other words, these enhancements up the ante on attackers while firmware remains the low-hanging fruit—the place where organizations have placed less effort thus far.

To date, the same security advancements have not yet been applied to firmware. To maximize return on investment, attackers can frequently find easy targets in firmware, which often runs older, vulnerable code with little to no protections. Since firmware is designed to operate without a lot of user interaction, it gets forgotten when we think about patching, configuration, or monitoring. Even more simply put, firmware is an often-invisible vulnerability which is harder to find and harder to fix, in many cases. Attackers go where the vulnerability is, and firmware is a good bet.

TAG Cyber: Isn't device-level security incredibly complex, especially if the enterprise doesn't have hands-on access to devices?

Eclipsium: Yes, it is. Firmware exists precisely because devices and the many components included in them are complex. In order to make devices easy to use, firmware abstracts this complexity for both users and operating systems. In some critical environments, physical techniques can be used to study and verify each component, but that requires experts who spend a long time

Indicators of confirmed implants usually call into question the rest of the hardware, and that device should probably no longer be trusted at all.



with each device and have intimate knowledge of each device type and component.

For most environments, we can give up some of this confidence to gain scale by automating checks in software. More or less, we use the same techniques in security tools that audit integrity, reputation, behavior, and configuration elsewhere in the software stack. For hardware devices, it takes experts to apply these to device-level assets, but once written, they can be reused everywhere.

TAG Cyber: Recent attacks have been propagated by signed updates from vendors in the supply chain. Given the complexity of firmware and hardware, how can organizations deal with supply chain risks across all the different manufacturers that go into a system?

Eclipsium: The supply chain problem cuts to the core of trust relationships inherited between organizations, making it extremely difficult to understand, let alone mitigate. I would consider two types of supply chain attacks. The first type of attack involves authentic deliverables that happen to be malicious. That overlaps quite a bit with the problem of either deliberate or unintended vulnerabilities and backdoors in firmware. Ultimately, we can architect to limit damage and monitor to track down and fix issues as they are discovered.

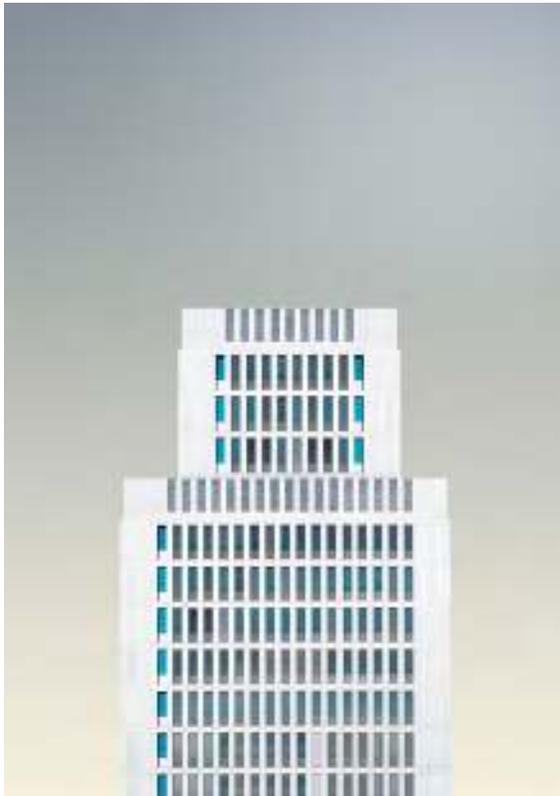
The other type of attack is some sort of modification or counterfeit that is not authentic. In this case, we can do various integrity checks on the device and its firmware. Both issues are present with great complexity throughout the software stack. The problem with firmware is that it adds yet another layer on top of everything else. To keep up, organizations need a risk management process that makes improvements in specific areas without the team becoming overwhelmed.

TAG Cyber: How does Eclipsium determine risk? What factors go into the assessment?

Eclipsium: Eclipsium focuses on what our customers need to do with firmware information so that they don't need teams of firmware and hardware security researchers to understand their devices and the threat landscape down at this level. We're automating that for them. We look at the impact and likelihood like anyone would, but we do it by combining multiple views of a device. We take direct measurements of each component (often using built-in capabilities provided by the manufacturer), but we cross-check against indirect behaviors or dependencies to form a "device profile." When we detect issues, we see this as a particular anomaly in the profile.

TAG Cyber: What happens, for instance, if an implant is found on an employee's device? How does that get fixed?

Eclysium: Generally speaking, a firmware implant should get immediate attention from security teams just like malware or physical access attempts—it's a focus on the potentially most damaging threats to an organization. Exactly what to do when something is found might be different depending on the specific organization or device, though. Indicators of confirmed implants usually call into question the rest of the hardware, and that device should probably no longer be trusted at all. Less severe issues usually fit into normal risk management or remediation processes like deploying updates, configuration changes, or monitoring for a period of time.





AN INTERVIEW WITH BRYSON BORT,
FOUNDER AND CEO, SCYTHE

USING EMULATION TO FIGHT AGAINST GRAVITY WITH LIMITED RESOURCES

Attack emulation has emerged out of the more well-known discipline of attack simulation, the idea being that creating a synthetic version of attacks and having defenders test their skills and tools against an artificial attack isn't sufficient to keep real attacks from penetrating defenses. While simulation mimics an attack, emulation duplicates real-life attacks and real-life vulnerabilities, borrowing from exploits in the wild and previously seen tactics, techniques, and procedures (TTPs).

The goal of attack emulation, or what can be known as attack detection and response, is to prepare defenders and help them keep pace with the massive number of vulnerabilities in systems and processes. SCYTHE, an adversary emulation platform, was built to help enterprise testing teams continuously assess their risk posture and exposure using automation and cyber threat intelligence. We recently spoke with Bryson Bort, Founder and CEO at SCYTHE, about this emerging technology space and how enterprises are leveraging their platform.

TAG Cyber: *Bryson, tell us a bit about the genesis of SCYTHE?*

SCYTHE: In 2016, the consultancy I had founded and was running, GRIMM, was approached by a Fortune 50 retailer. They truly had built a world-class cyber security program. They asked us to build a custom implant because the problem they had come across was how to test the edges of a program at that level. I realized that they had defined a market need, because going to a third-party consultancy for a custom build is your plan of last resort—it is quite costly and time consuming, generally speaking. Nonetheless, we accepted the work and I went back to the company with the idea of building a modular platform that would be infinitely extensible and would work at scale. We spent two and a half years refining it in their environment with our internal R&D program before we went to market at the end of 2018.

TAG Cyber: *There are plenty of security testing and vulnerability assessment methods. Why did you feel these activities, either standalone or in combination, weren't enough?*

SCYTHE: Per our origin story, the assessment market had been a monoculture for a long time, driving the de facto solutions that the security community had built around. Security assessments were the domain of specifically trained professionals and were mostly limited engagements due to resource constraints—time, staff, and money.

The automated testing tools that have come to the market since only address the technical aspects; however, we know that the largest surface area of risk involves people.

**In this industry,
we're really good
at learning and
solving yesterday's
problems, only to
be surprised yet
again tomorrow
by some new tactic
or technique.**



Security is a constant fight against gravity with limited resources: You have to continually validate people, process, and technology to maintain the progress your team has made. People don't scale, but tools do.

TAG Cyber: SCYTHE's platform looks great for larger enterprises with established red, blue, and/or purple teams. What about smaller companies without the in-house skills, how can they test their defenses?

SCYTHE: Our market approach brings three elements together: partners, enterprises, and the small and medium-sized businesses, SMBs. Partners are the professional consultancies that provide third-party risk assessments; they power the platform's development of what it can do at the edge. Enterprises are the upmarket solution with requirements for a whole of team approach involving scale, flexibility, integration, and automation. Then, we combine both of these elements into automated packages, what we call our Threat Catalog, that can be automatically run to gain baseline insights and metrics.

We also have an internal services arm that is very affordable for clients who want or need professional support. Plus, we have partnered with a number of MSSPs to offer these services to small businesses that already have a relationship with a security services provider.

TAG Cyber: Why is emulation necessary? Are attackers gaining more skills? Are companies getting worse at proactive protection?

SCYTHE: In this industry, we're really good at learning and solving yesterday's problems, only to be surprised yet again tomorrow by some new tactic or technique. Emulation is necessary because security teams need to work against and learn from a realistic attack chain to focus on the detection, response, and remediation of behaviors of real, human adversaries, versus working from a checklist. The focus on behavior allows companies to be a little more ready for tomorrow's attacks than they are today.



TAG Cyber: Everyone in security knows about MITRE ATT&CK, PTES, and other recognized industry frameworks. What are some regulatory frameworks and methodologies that enterprises will benefit from in their testing efforts?

SCYTHE: There are a few I recommend:

- G-7 Fundamental Elements for Threat-Led Penetration Testing: The Group of 7 nations provided guidance on performing threat-led penetration testing.
- CBEST Intelligence-Led Testing – Bank of England: This is a regulation for financial institutions operating in England.
- Threat Intelligence-Based Ethical Red Teaming – TIBER-EU: This is a framework that can be leveraged by any country in the European Union and offers cross-jurisdiction and mutual recognition of red team engagements.
- Red Team: Adversarial Attack Simulation Exercises – ABS (Association of Banks of Singapore): This is focused on financial institutions in Singapore.
- Intelligence-led Cyber Attack Simulation Testing (iCAST) – HKMA (Hong Kong Monetary Authority): This is focused on financial institutions in Hong Kong.
- Financial Entities Ethical Red-Teaming – Saudi Arabian Monetary Authority: This is focused on financial institutions in Saudi Arabia.
- A Framework for the Regulatory Use of Penetration Testing and Red Teaming in the Financial Services Industry – GFMA (Global Financial Markets Association): Given all the country-mandated regulatory requirements, the Global Financial Markets Association set off to create a global framework that would meet multiple countries' regulatory requirements.

Whether or not your company falls under the country-specific frameworks provided above, each one includes guidance that can be applied to any organization that wants to enhance its security posture through improved testing.



AN INTERVIEW WITH JASON CLARK,
CHIEF STRATEGY OFFICER, NETSKOPE

CONTEXTUALIZING DATA PROTECTION WITH SASE

The secure access service edge (SASE) is becoming a hot topic that refers to the integration of cloud security and networking, delivered at the edge and at scale. While not yet a clearly defined market, many solution providers with histories in cloud security and software-defined security are looking at how to combine capabilities, improve upon them, and give their customers better visibility and control of cloud-based resources.

During the past year, as work from home took hold in an unprecedented way and spurred on even greater cloud adoption, the need for SASE (pronounced “sassy”) has never been more urgent. Netskope, with its nearly 10-year proven track record in network and cloud security, has been making great strides in the SASE market, including its CASB, zero trust network access, and next-gen secure web gateway.

The TAG Cyber analyst team recently spoke with Jason Clark, Netskope Chief Strategy Officer, about what it means to be a SASE platform provider and where the cloud security market is headed.

TAG Cyber: *No company starts off as a SASE platform, but SASE is the big push at Netskope at present. What drew the company toward this approach to cloud security?*

Netskope: There’s a lot of what we might call “SASE-washing” out there. It’s similar to what we’ve been seeing with zero trust for a decade now; the more popular the term SASE gets, the more every vendor with even passing relevance to cloud security or networking wants to attach to it and do marketing around it.

For Netskope, however, SASE is a natural fit for the vision we’ve been sharing since our earliest days. The biggest fundamental shift with digital transformation is that data is no longer on a CPU that the enterprise owns. Security teams must invest in the right technology to achieve more complete data protection, and we all need to ensure zero trust principles are applied everywhere data needs protection.

Well-designed SASE is really about the evolution of data protection. Modern data protection, in turn, is ultimately about context. By monitoring traffic between users and apps, including API traffic, we can exert granular control. We can both allow and prevent data access based on a deep understanding of who a user is, what they are trying to do, and why.

At Netskope, we’ve been describing this approach as Zero Trust Data Protection, and we think it’s a critical differentiator between true SASE and quote-unquote “SASE.” Think about it: Knowledge of the interplay between user, device, app, and data enables security teams to define and

Well-designed SASE is really about the evolution of data protection. Modern data protection, in turn, is ultimately about context.



enforce conditional access controls based on data sensitivity, app risk, user behavior risk, and other factors. The result is more effective security overall via continuous risk management.

TAG Cyber: Zero trust was envisaged to apply protection in a perimeterless world. How does SASE further the idea of perimeterless security?

Netskope: In an era where the cloud rules infrastructure, traditional network security needs to transition to the cloud. As organizations go through their digital transformation journey and move into the cloud, they're leaving behind the traditional perimeter of their data center. Using a SASE approach allows organizations to apply granular security controls at the edge of their network, closest to the user, applying protection regardless of where or how they access sensitive data.

TAG Cyber: What are the market drivers behind SASE adoption?

Netskope: Efficiency, cost savings, and better protection for a remote-heavy workforce—all without sacrificing user experience. By embracing SASE to create a secure network edge, enterprises can better address an increasingly remote workforce and the migration of apps and data to the cloud. This allows organizations to reduce their reliance on costly, legacy WAN architectures with their complex routing, extensive traffic “hair pinning” or backhauling, and the added latency that comes with these architectures. Ultimately, these legacy approaches lead to sacrifices on performance for the sake of security, which ends up slowing down business and impacting productivity.

TAG Cyber: What kind of companies, and what job titles within those companies, are showing the most interest in a SASE solution, and why?

Netskope: What's inspiring is that to get to a true SASE solution, networking and security functions will need to converge. Network and security professionals have been at odds for a long time and focused on different things. But successful SASE and its benefits depend on how well networking and security can come together to achieve mutual goals around uptime, experience, and data protection. It's remarkable when we can get this right; everyone from security analysts and CISOs to architects and VPs of infrastructure will be better aligned and more productive, not siloed.

TAG Cyber: Tell us a little about the Netskope Security Cloud and what capabilities it combines.

Netskope: The Netskope Security Cloud provides a single pass security cloud for user traffic including websites, managed apps, unmanaged apps, public cloud services, and public cloud custom apps. Forward and reverse proxies support any user, device, or location. Managed apps also benefit from API

inspection of data-at-rest for data and threat protection. Remote users benefit from zero trust network access (ZTNA) to private apps within the cloud or private data centers. Cloud security posture management (CSPM) provides continuous security assessments for IaaS, including for compliance regulations. The net result is the consolidation of SWG, CASB, ZTNA, DLP, ATP, and CSPM capabilities in one single pass security cloud.

Built from the start in one cloud, Netskope has the industry's only next-gen secure web gateway (NG-SWG) solution that has unified a market-leading inline CASB with a cloud secure web gateway and advanced cloud DLP—all from a single platform and administered from a single console.

No other cloud security vendor can do what we do, especially when it comes to data protection in the cloud. Many of the biggest and best-known organizations in the world are now trusting us to be their partner of choice for secure digital transformation.





**ANALYST
REPORTS**

Protecting Digital Identity from Cyber Compromise

Prepared by

Katherine Teitler
Senior Analyst, TAG Cyber
katie@tag-cyber.com

COMMISSIONED BY



Introduction

Day in and day out, a vast array of software and services contain the data and applications that businesses rely on to keep the wheels turning. Twenty-five years ago, a business could operate efficiently without heavy technology use. Today, it would be next to impossible.

Efficiency gains from digitalization have, without a doubt, accelerated the pace of business and increased opportunities for product development, global expansion, and revenue growth. However, a downside to this hyper growth is the 24x7 access to sensitive and proprietary information by cyber criminals. To combat this, cyber security practitioner and vendor communities have expanded, with a relentless focus on finding, stopping, and mitigating cyber threats. A layered approach to cyber protection necessitates security control throughout the OSI stack, but one common denominator stands out above the rest as a leading facilitator of cyber incidents: identity.

There's an adage: *On the internet, nobody knows you're a dog*. It was published in conjunction with a cartoon in *The New Yorker* in July 1993.¹ It was also the first time popular culture recognized the potential for digital stealthiness. It was foreshadowing of what many in security know to be true today; bad actors take on unsuspecting identities to get into an organization.

Since the cartoon ran, identity has become the "new perimeter" and access controls must incorporate identity governance to be effective. Without any way to understand and validate identity—of humans or machines—organizations have little chance of reducing the potential for cyber attack.

This is exemplified by the shift in control of identity and access management from an IT function to one wholly or largely governed by security teams. In a recent survey of 262 IT and security professionals, 95% of respondents said their company maintains a formal identity and access management program with dedicated resources and budget, and which falls under or has a dotted line to the security program.

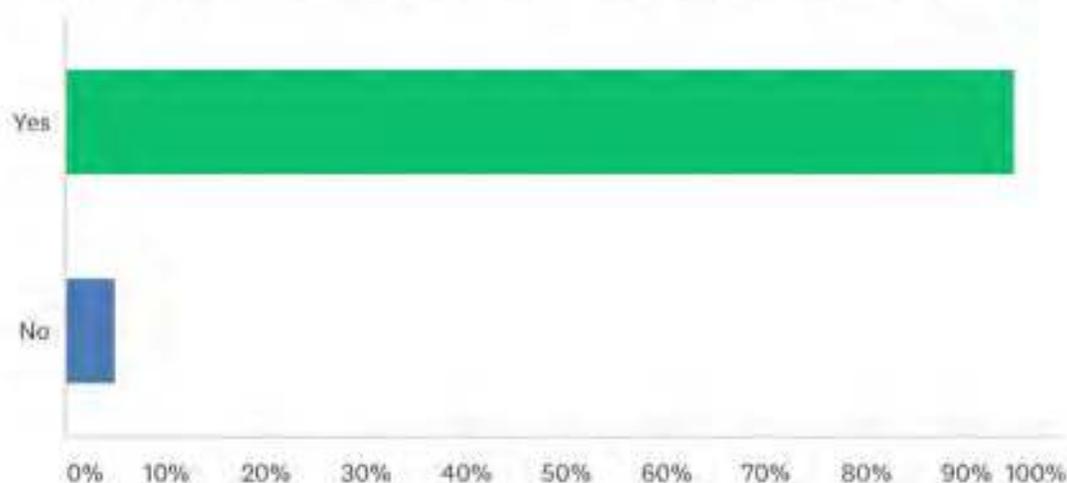


Figure 1. Percent of companies with a formal IDAM program which falls under or has cyber security governance

This is a significant change from just a few years ago when identity and access management (IDAM) was merely a matter of IT teams provisioning access to resources. Today, identity and access are much more complicated, triggered by the number of entities on or connecting to a network and the myriad types of networks used across organizations.

The implications of considering IDAM a security control are numerous. Most prominently, identity is not stagnant. Like when a person can change their physical identity: clothing/accessories, hair style and color, and where they are physically located, digital identities, change constantly, potentially even more so when it comes to applications/software. This means that authorization and authentication must be predicated on more than what something appears to be and must account for constant change.

“Authorization and authentication must be predicated on more than what something appears to be.”

In addition, identity, especially identity based on fixed parameters, cannot be the sole control for access. Unmanaged or improperly managed identity is a leading cause in cyber security incidents. This is

because “identity” is not straight-forward in the digital realm due to constant changes. Yet, because so much of the access required by humans and machines is based on verification of a positive ID, it is imperative for businesses to get right.

Demographics

TAG Cyber surveyed 262 technology professionals about identity-based cyber security incidents. Forty percent of respondents are IT managers/directors, 29% are security managers/directors, and the remainder are spread across security- and IT-related categories.

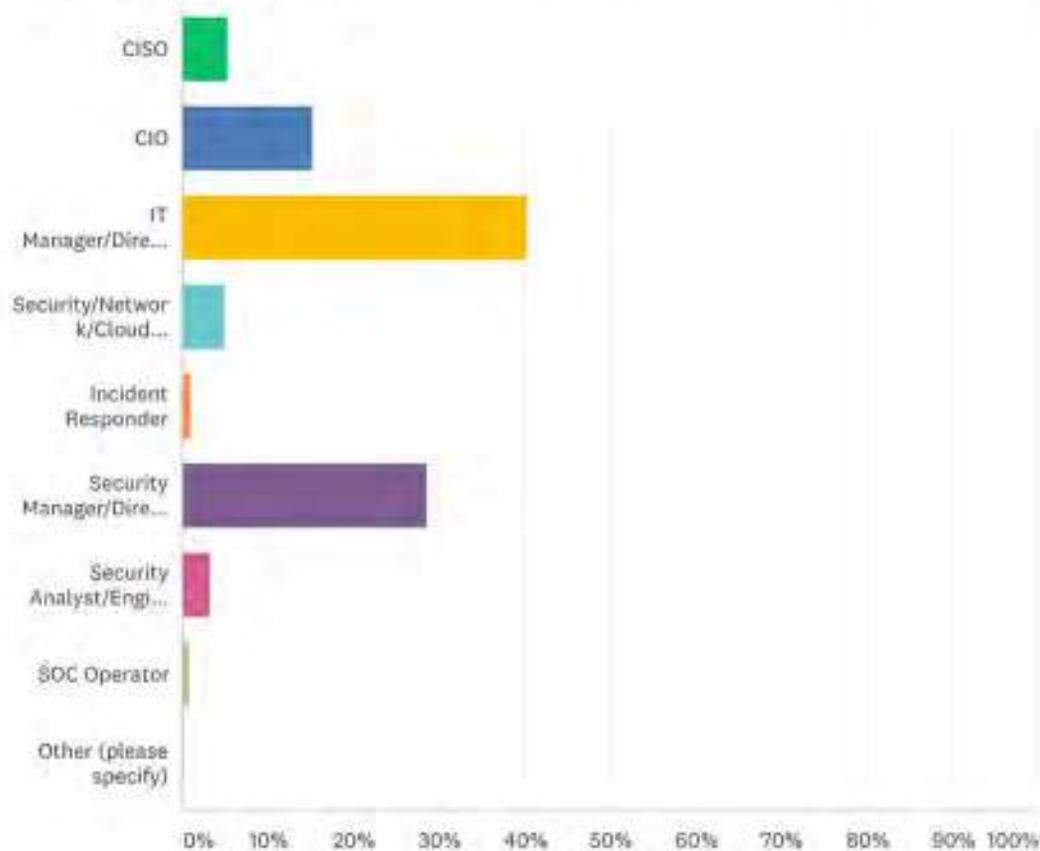


Figure 2. Survey respondents' job titles

The industries represented in the respondent pool are similarly diverse. The top five industries represented are computer manufacturing (hardware, software, peripherals), computer and networking services/consulting, information technology (the write-in for "other"), internet/application service provider, and data processing services. Banking and retail tied for sixth place.

Thirty-four percent of individuals surveyed work for large enterprises (more than 10,000 employees), with 21% working in companies with 50,000+ employees, and 66% of respondents work for medium-sized businesses. Companies with fewer than 500 employees were not considered for this survey.

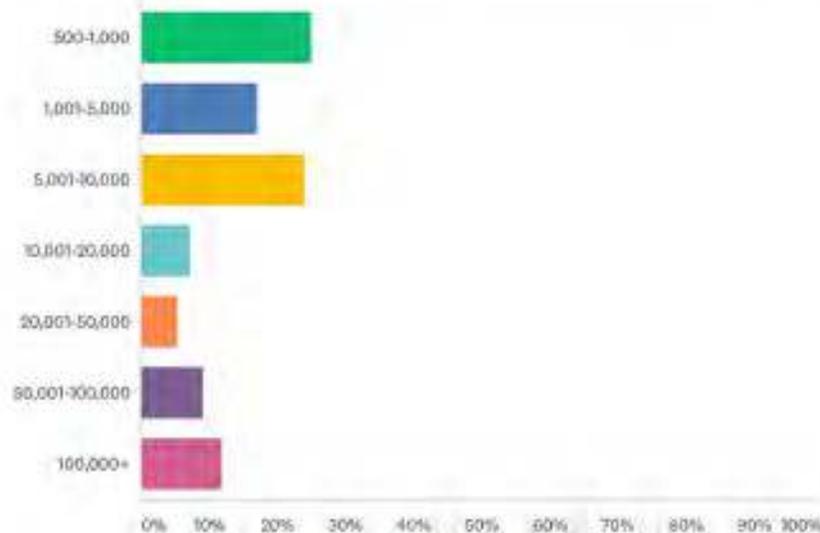


Figure 3: Company size

Prevalence of identity-based problems

Now to the heart of the matter. 100% of survey respondents answered "yes" to the question, "To the best of your knowledge, has your organization experienced a security compromise in the last year?" Further, 83% said the compromise(s) included unauthorized access to identity information, including that of employees, partners, contractors, and customers.

This is a poignant point because it underscores the necessity of understanding and appropriately governing identity-based controls in the enterprise. It also reinforces the fact that even large, well-resourced enterprises have enough trouble managing identities such that lack of control and/or visibility facilitates security compromise.

"100% of survey respondents answered "yes" to the question, "To the best of your knowledge, has your organization experienced a security compromise in the last year?"

Volume

As for how many identities have been compromised via these security events, 35% of respondents say the number is between 1-10,000. On the other end of

the spectrum, 32% of respondents said 1 million or more identities were compromised in the past year.

Identity compromise significantly leads to larger-scale cyber attacks, and considering the average cost of a lost/stolen data record is \$146 USD,² companies must place greater priority on implementing identity-based access controls. The aforementioned cost doesn't

necessarily even account for additional security controls a company would need to procure and implement after a compromise, the reputational damage that might follow a public breach, or any customer churn resulting from mishandling or lack of control over identities.

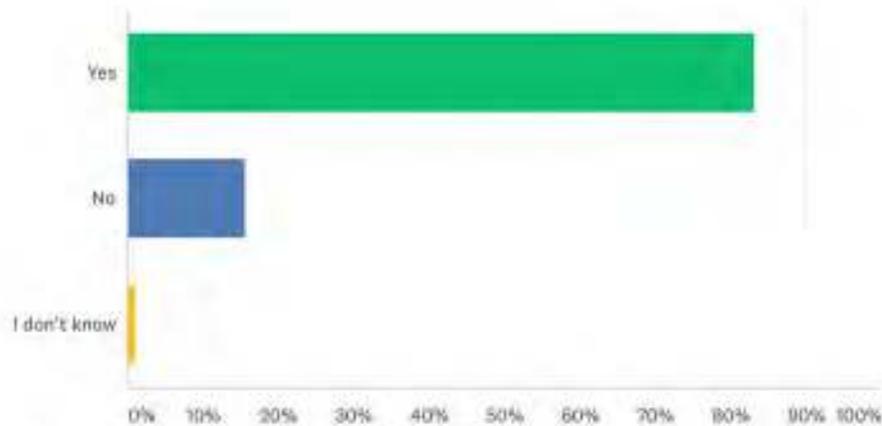


Figure 4: Percent of companies with an identity-based compromise in the last 12 months

Permissions and provisioning

If the sheer number of compromises weren't only cause for concern, 71% of respondents admitted that compromised identities led to unauthorized access to data that should have been deleted or destroyed. Credit card records for one-time transactions and unnecessary PII (e.g., birthdates, race, religion) are examples of excess data often collected by companies but which are commonly unnecessary for day-to-day use. Nonetheless, storage of this data raises risk exponentially.

Further, 75% of respondents said that the compromise(s) were facilitated by over-entitled/over-permissioned access. Excessive permissions and entitlements are a major cause of data breach, primarily because understanding the entirety of a company's data,

devices, systems, and software is challenging due to its relentless expansion and growth.

Fewer respondents (66%) said identities that should have been inactive were compromised during the security incident. This means identities of former/ex-employees, contractors, past partners, etc. provided a pathway to compromise that could have been prevented if the company had a better, perhaps automated, way to see and manage identities and access controls. Especially when it comes to cloud governance, security teams of all sizes and maturity report trouble keeping up with the various controls required for different platforms, user permissions, and ephemeral workloads.

"71% of respondents admitted that compromised identities led to unauthorized access to data that should have been deleted or destroyed."

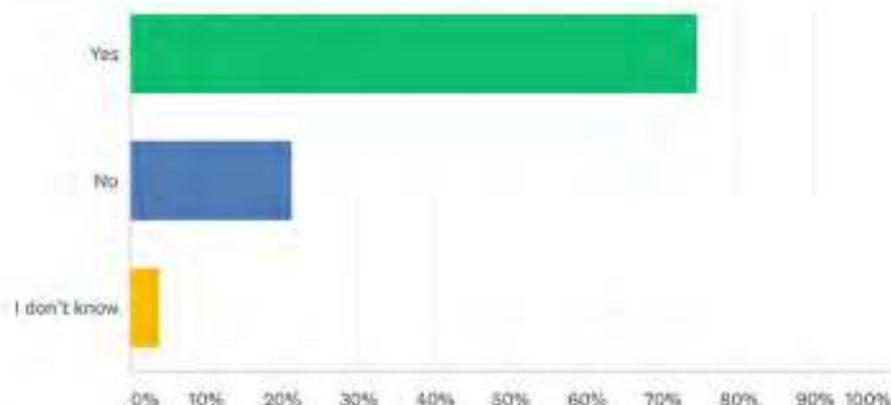


Figure 5: Percent of respondents who say compromised identities had excess or unnecessary permissions

Security teams must get out in front of the problem by deploying the right tools and processes which provide continuous assessment of who or what is accessing every endpoint/system/record/applications. Doing so will significantly reduce the unauthorized access that results in compromise. While an asset inventory or management program is helpful here, that's only the starting point; it's access that is of prime importance, and that's governed by identity.

"It's access that is of prime importance, and that's governed by identity."

Incident identification

In the past, most compromises were reportedly first discovered by external entities like law enforcement or partners. According to our survey, even though identity compromise is a notable vulnerability, companies are getting better at internally identifying compromises.

The category choices were as follows: external notification from law enforcement or partner; internally discovered – alert from security tool; internally discovered – unusual identity behavior; internally discovered – proactive hunting; other.

When digging deeper, there are interesting nuances to the responses. For companies with 1,001-5,000 employees and companies with 10,001-20,001 employees, the balance between internal and external discovery was essentially even.

For companies with employee counts of 5,001-10,000, 50,001-100,000, and 100,000+, the number of internally discovered incidents was roughly twice that of discovery by an external source.

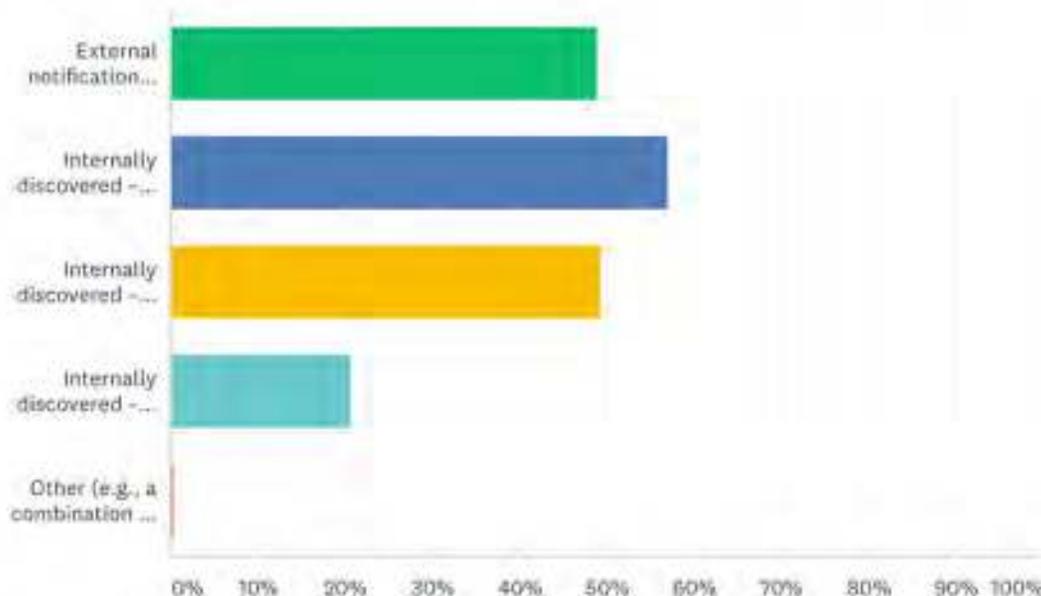


Figure 6: Question: How was the compromise first discovered? If more than one compromise, select all that apply¹¹

For companies with 20,001-50,000 employees, 2 ½ times the discoveries were via internal resources.

For the smallest companies in our survey—500-1,000 employees—external discovery was 5% more than internal discovery, and only 12 of those companies said they'd used proactive hunting to identify a compromise.

From this data, we can conclude that the midmarket up has made substantive strides in internal detection over the years—which is preferable since it's likely to be faster than waiting for the FBI to call.

Conclusion

On the whole, businesses are improving their ability to detect cyber intrusions and compromises, even in the face of growing complexity, network sprawl, and increased cloud usage. However, identity-based compromises continue to plague organization across every industry sector and company size. But this does not have to be the case. Companies can protect digital identities with identity governance and hardened identity and access management tools.

On a positive note, more companies have formalized identity and access management programs so that they either fall under or have governance from cyber security teams. This is a positive trend, as identity-based compromises can result in numerous problems: data breach, malware injection, network outages, data loss, compliance violations, and more. Problems: data breach, malware injection, network outages, data loss, compliance violations, and more.

“The recommendation is for security teams to implement technologies that allow them to gain greater visibility and control.”

The recommendation is for security teams to implement technologies that allow them to gain greater visibility and control over identity provisioning, access requests, password management, policy management (including least privilege), and separation of duties, using zero trust principles. Automation and machine learning are critical elements, too, as the principles. Automation and machine learning are critical elements, too, as the management of identities is too onerous and dynamic for individuals to manage manually.

Given the resource constraints of security personnel, manual identity management is a waste of time; security teams must deploy technology that can efficiently and effectively manage identities—from provisioning to setting appropriate, roles-based policies to deprovisioning—throughout their entire lifecycle with little administrative burden.

ⁱhttps://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-pete-r-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html

ⁱⁱ<https://www.ibm.com/security/data-breach>

ⁱⁱⁱCategory choices: external notification from law enforcement or partner; internally discovered – alert from security tool; internally discovered – unusual identity behavior; internally discovered – proactive hunting; other

Maximizing Open Source Security Tools by Engaging an Open-core Vendor

Prepared by

Adam LeWinter
Senior Analyst
adam@tag-cyber.com

Introduction

Open source security solutions provide fantastic data capture capabilities that provide critical data to security operations teams. They provide security expertise beyond a single vendor's engineering team by benefiting from developers around the world who contribute to the projects and help corporations avoid becoming beholden to any vendor.

Every great open source project thrives because the source code is developed by individuals who are not working for a single vendor, not beholden to the economic or technical constraints of that vendor, and because open collaboration allows for the development of more powerful software more quickly. The most successful open source projects have a large community that actively supports the project. Community developers are very engaged and often motivated by a desire to solve a specific problem, disrupt a commercial space, remove the need for vendor lock-in, or the recognition they get from their peers. This leads them to be invested in the success of the project and make high quality contributions, which in turn results in most established open source projects being relatively bug free and feature rich.

However, nothing comes for free, even if there is no license cost. The cost of implementation, ongoing maintenance, and tuning to get useful information integrated into core security tools are costs that are often overlooked when deciding to adopt an open source solution. A commercial open-core vendor removes the unknowns that come with implementing open source solutions and ensures their success when it matters most while still benefiting from the global contribution and avoiding vendor lock-in.

In this report, we investigate an open source network monitoring project called Zeek as a foundation to illustrate how open source solutions provide fantastic information to security operations teams, but may be best consumed via a commercial "open-core" vendor to maximize the value of the technology.

What is Zeek?

Built by Vern Paxson in the 1990s when he was a graduate student at UC Berkeley, and formerly known as Bro, Zeek was developed as a passive network traffic analyzer to understand what was happening on his university and national laboratory networks. Today, Zeek supports network security operations at a broad variety of sites, including major corporations, universities, research labs, and supercomputing centers. Zeek is primarily used as a security monitor enabled by sensors running on commodity hardware on standard UNIX-style systems and provides telemetry data extracted from live network traffic. The network traffic examined by Zeek is out-of-band, typically a live copy of primary traffic provided through a packet broker, or via a tap / span. The stream of traffic is processed by Zeek's real-time event processing engine that analyzes it using policy scripts to generate events, which are then written to event logs. See Figure 1.

¹ <https://zeek.org/>



Figure 1. Zeek Architecture²

These logs include a comprehensive record of every connection seen on the wire across multiple network protocols. Zeek also captures application-layer specifics such as HTTP session information, DNS requests and replies, SSL certificates, and content of SMTP sessions along with data from dozens of other protocols. Zeek logs are well-structured, tab-separated log files and are commonly sent to external systems like a SIEM for post-processing and analysis. In addition, Zeek can extract and reassemble more than 200 types of files for file analysis and offers a Turing-complete programming language that the open source Zeek community has used to create and share hundreds of custom behavioral analysis scripts (Zeek packages), such as the JA3 / JA3S script that can fingerprint TLS traffic.

Why Choose Zeek?

Zeek has become one of the most popular network monitoring solutions available with its comprehensive data stream and flexible scripting platform. What sets Zeek apart from classic intrusion detection systems (IDS) is its neutrality. Zeek does not try to determine whether traffic is benign or malicious, but simply observes and captures network traffic from a security point of view. Zeek data can be invaluable in the event of a breach and provide either real-time or historical data critical to the investigation and remediation efforts. Zeek's extensible and customizable platform provides a scripting language to allow users to do custom, tailored analysis rather than being limited to a set number of hard-coded signatures or behaviors. This Turing-complete scripting language allows users to go beyond classic signature-based detections and allows users to define their own approach to finding anomalous activity based on behaviors, inferences, and insights.

Zeek does provide built-in analysis and detection functionality for basic security events such as IDS-style pattern matching, reporting on vulnerable versions of software, application identification, validating SSL certificate chains, and detecting SSH brute-forcing. However, the focus for Zeek is to provide a platform that facilitates analysis and allows users to define their own approach to finding anomalous activity.

Zeek can be installed in almost any environment to provide an immediate view of network activity. Zeek is also designed to be scalable with a cluster architecture that can support 100GE networks by utilizing load-balancing and a centralized management platform that coordinates and synchronizes instances across the cluster.

And from a monetary perspective, like all open source projects, Zeek has no license cost which makes it an attractive option for corporations looking to enhance security capabilities without requiring additional budget. However, while open source software might be free from a license perspective, there are real costs that teams must consider when implementing.

²<https://docs.zeek.org/en/master/intro/index.html#architecture>

Challenges to Open Source

As we have discussed, Zeek is an open source solution with a lot of useful functionality and benefits for corporations, governments, and universities. The monitoring and analysis platform is flexible and provides a license-free alternative to proprietary solutions. However, open source solutions do have some challenges to be considered.

The challenges associated with open source software have real costs. The flexibility provided by an open source solution like Zeek also means that myriad options exist when it comes to deployment and customization. Looking at a typical Zeek deployment, a user must first choose the correct hardware integrated with an appropriate network interface card on which to run the Zeek sensors. Then a Linux OS must be installed on the hardware followed by the installation and configuration of Zeek and any needed custom or third-party packages. Once all the software is installed the system needs to be tuned and any issues, such as packet loss, need to be debugged. A monitoring solution for the sensors needs to be configured and the output from Zeek needs to be integrated with the organization's security analytics toolset, such as a SIEM. This initial installation process can take a lot of working time. Once operational the Linux OS, Zeek software, and any add-ons need to be upgraded for new features and patched over time to deal with any unforeseen issues.

Organizations with limited IT teams and resources may not have the time or desire to customize and tune the solution to fit their needs. Even those organizations with the necessary resources face an opportunity cost when their highly skilled security employees must spend their limited time on open source deployment and maintenance instead of front line work. In the case of Zeek, the specific people who are likely to have built, deployed, and are responsible for maintaining the Zeek sensors are the very same people who are also responsible for incident response and threat hunting. Every hour, day, or week they spend on system administration is time lost to their actual mission critical job of defending their organization's network and infrastructure.

Additionally, community knowledge bases may not have answers to questions or issues specific to the organization's environment, and there is no technical support other than best efforts from the community. The time required to troubleshoot and fix any issues can quickly become an expensive operational cost and time sink that prevents employees from doing their primary job.

While there are no immediate license costs with open source solutions, these follow-on hard, soft, and opportunity costs incurred in deploying, tuning, and maintaining an open source solution can become expensive. Organizations looking to adopt an open source solution should therefore look for a solid partner or commercial vendor that can provide a solution based on the underlying open source technology while removing some of the inherent operational complexity. Commercial vendors also often provide prebuilt deployments, services, support guarantees, and enhancements on top of the open source components which allow corporations to maximize the value of the open source technology.

Strong "Open-core" Vendors Reduce Costs of Open Source Solutions

In general, open source solutions can be expensive to scale to the operational needs of an organization without the partnership of a strong open-core vendor. A vendor can minimize the effort required for the initial deployment as well as the continuous maintenance issues faced when implementing an open source solution. The vendor can also provide best practice guidance on how to be successful in the specific environments and architectures that exist within the organization. This expertise reduces the costs of implementing an open source solution by limiting the time invested by security operations teams.

While engaging with a vendor typically incurs a license cost, vendors allow organizations to reduce the unknown ongoing operational costs of running an open source solution. Once installation is successful and data is being collected, teams must then tune what data they receive and in what format. Given that each environment in the organization can utilize different technologies, the 400 fields Zeek sensors collect about the network need to be distilled down to a set of relevant fields for each unique environment. A vendor will often have support for these environments with prebuilt best practice implementations that remove the need for a security operations team to invest time re-inventing the deployment and tuning for each environment within the organization.

Another benefit of having a commercial vendor is that the implementation is not dependent on the knowledge of a single person. Vendors support a wide variety of corporations in multiple verticals which allows them to accumulate knowledge about common requirements, issues, and ways to get the data to teams that need it. Not every security operations team will utilize the same SIEM, SOAR, and other operational tools, and each tool has its own expected format required of the data. The time required to format the data in a way each tool can ingest can be a lengthy process that a vendor will have already completed and be able to provide with limited additional effort.

The time required for deployment and implementation can also limit the effectiveness of an open source solution like Zeek. The network data provided is a great way to enhance a SIEM or SOAR platform, but if it is not tuned correctly and continuously for the environment, it can make things worse rather than aiding in a solution during an incident. During an incident, most security teams eventually want to turn to network data as a complement to other sources, like endpoint data, to get a full understanding of what is happening or has happened. If the network data is incomplete or unavailable, it can severely hinder a security team's ability to respond quickly. Having a partner to help ensure complete installation, best practice data collection, and effective data integration into core security tools removes the risk of using open source solutions and allows the solution to provide value when it is needed most.

Conclusion

From the flexibility they provide in terms of customization, to the quality benefits they offer by having multiple people checking for bugs and fixing them, the advantages of open source software have often been written about and discussed at length. However, there are also some considerations that should be made when investigating whether an open source solution is the best solution for a corporation or government agency.

While open source solutions might be license free, they often incur high operational costs in maintenance, tuning, and support which can lead to unneeded risk in corporate environments. The best way to minimize this risk is by engaging a commercial open-core vendor who can provide knowledge and support on top of the benefits open source solutions provide. Open-core solutions also avoid the high cost of having to rip and replace solutions because if you are no longer happy with a commercial product or service built on top of an open source technology, you can simply stop paying the vendor and continue to use the underlying technology. Commercial open-core vendors remove the risks that come with relying on open source technologies while still allowing corporations and government agencies to benefit from the global contributions and avoid vendor lock-in.

Packet Capture is a Foundational Technology

Prepared by

Adam LeWinter
Senior Analyst
adam@tag-cyber.com

Version 1.0
April 2021

Introduction

As distributed applications and cloud services have become commonplace, the increased complexity in network and application architectures has made it challenging for teams to ensure the reliability, performance, and security of enterprise networks. These complex environments open more attack vectors for exploitation while making it difficult or impossible for security teams to quickly determine what has happened in the event of a security incident. This has led to the need for organizations to capture complete information about network activity and provide it to security teams as a critical resource for enabling timely remediation and avoiding costly outages or breaches.

The success of network security monitoring and threat detection is directly related to the ability to accurately capture network traffic. The importance of packet capture is often overlooked for newer security analytics tools utilizing artificial intelligence or machine learning. While most of these newer tools utilize some (typically limited) packet capture capabilities to provide data for their analytics, the packet data is discarded once it has been analyzed—except for maybe a handful of packets to show what triggered the alert. These tools are not designed to capture the traffic, index it, and store it for use in historical investigations of the network.

Analytics tools are great at detecting anomalous behaviors, but it is often a challenge to use them to quantify a breach and its impact. Understanding the depth and breadth of an attack, what data has been lost, and how to fully remediate an incident is something that requires more network context than can be found in a handful of packets. Visibility is the bedrock on which security teams operate and a strong packet capture solution provides the network visibility data to enable security teams to prevent, investigate, and remediate security incidents.

“Visibility is the bedrock on which security teams operate and a strong packet capture solution provides the network visibility data to enable security teams to prevent, investigate, and remediate security incidents.”

While most security teams and network administrators turn to packet capture as the source of truth when investigating incidents, they often only turn on full packet capture after an incident has occurred. Packets can only be captured as they traverse the network, so the selective approach of using a packet sniffer after an event misses crucial data during the actual incident and causes gaps in the historical record.

Triggered packet captures based on alerts can also miss crucial data as threat actors are often able to lurk undetected in networks for weeks or longer before an alert is triggered. Continuous, always-on packet capture provides the historical network data that enables accurate threat detection, investigation, and response, and allows security teams to take a more proactive threat hunting approach.

Packet Capture is Foundational in Security Programs

TAG Cyber classifies packet capture as part of the network monitoring control which has always been a core component of cyber security architectures. In modern cyber security infrastructure TAG Cyber defines two primary functional requirements for network monitoring— (1) the ability to collect data at large capacities in the 100 Gbps and above range and (2) the ability to process the collected data at line speed to detect indicators of compromise. Packet capture satisfies these requirements because it provides the necessary data at line speeds from large bandwidth capacities that enables the analytics. Packet capture also conforms to the NIST 800-53 v5 framework—specifically the Audit and Accountability (AU) control area which details logging and retention requirements—by providing data necessary to audit compliance standards.

The increase in encryption of network traffic has increased the challenge for many monitoring solutions to fulfill these requirements and provide the necessary data and analytics. While encryption does limit the data that can be required, it is possible to glean useful information from encrypted traffic as packet headers and the TLS conversations provide useful data without requiring access to unencrypted payloads. However, packet

capture solutions provide the best value when attached to a TLS proxy at the perimeter of the network capturing decrypted traffic and storing it securely. The visibility provided by a packet capture solution at the perimeter provides the ability to detect attacker communications outside of the network such as data exfiltration and command and control behaviors.

It is also important to note that usually not all segments of a network are encrypted as network operator visibility or performance sensitivities may require unencrypted traffic in some cases. Environments can also be architected using the idea of secure enclaves where decrypted traffic within the enclave is available for inspection by security tools.

“Continuous, always-on packet capture provides the historical network data that enables accurate threat detection, investigation, and response, and allows security teams to take a more proactive threat hunting approach.”

Therefore, teams should consider if and where there is a need for analyzing or recording encrypted traffic and if a network monitoring solution with decryption capabilities is needed.

Collecting and analyzing data from the network will remain a staple of cyber security programs as it provides a foundation for much of the work performed by a security operations center (SOC) and provides the data required for auditing of compliance standards.

Requirements for Packet Capture in Modern Architectures

There are a few key features that are needed when looking at implementing a packet capture solution in modern architectures. Packet capture solutions need to be able to capture traffic without packet loss and store complete network history to be effective. A complete network history is crucial to the effectiveness of teams when responding to any incident as attackers often have long dwell times in environments before triggering alerts. Security incidents can occur at any time and having incomplete or inaccurate network data adds unnecessary complications and can make it impossible to effectively respond. Without the packet payload a security team might be able to deduce a breach happened, but it will be difficult to impossible to determine what data may have been exfiltrated. Always-on packet capture allows teams to look through the network history to find attacker behaviors, such as lateral movement and command and control, which allows teams to understand the breach impact and identify impacted data assets. This is particularly important with regulatory obligations that require affected stakeholders to be notified in the event of a breach, often within very tight timeframes (72 hours with GDPR).

Always-on Packet Capture

Packet capture solutions also need to be always on and recording. Ad hoc or triggered capture fails to capture critical data because it is impossible to predict what packet history will be needed when performing an investigation. Packet data can only be recorded as it flows through the network and any dropped or missed packets force security teams to try and reconstruct events from log files or NetFlow data which is a slow and cumbersome process that often leads to inconclusive results. Capturing all the packet data means critical data is always available when teams need to reconstruct past events and is only limited by the depth of history that is stored.

Lastly, packet capture solutions need to provide fast access to packet data. The ability to integrate that data into a wide range of third-party security tools (commercial, open-source or custom) from IDS/IPS, SIEMS, SOAR, to AI/ML-based tools, is crucial. Analysts need fast access to packet data from the tools they use to do their job. Search and data-mining operations need to provide access to specific packets of interest relating to a specific event quickly – which means sifting through petabytes of distributed packet history. The faster this can be done, the more productive analysts can be, and the faster they can respond to threats to minimize their impact.

Implementing Packet Capture in Modern Architectures

While these requirements may seem obvious, the overall complexity of modern environments makes it non-trivial. There are ever-increasing numbers of pathways for network traffic as the average number of applications in environments continues to grow. The volume of traffic also makes packet capture a challenge as most networks now see 10Gbps usage or higher, making capturing accurate details for each packet very hard.

This means the ability to scale with the needs of the network is at the core of any data capture implementation. As network links get faster and larger it is becoming more important that packet capture solutions support higher throughput networks. Scaling up storage, computation capabilities, and search performance across an ever-increasing set of network data is what makes a packet capture solution feasible.

Insufficient data retention leads to intermittent capture of network events and makes reconstructing network flows impossible during investigations. Providing users the ability to cost-effectively store more network history gives analysts the ability to go further back in time to accurately reconstruct and analyze events days, weeks, or even months after they have happened.

Historically this scale has come at a high cost which has limited implementations from being able to provide always-on capture. However, reductions in storage costs combined with cost-effective distributed storage approaches, intelligent data truncation strategies to avoid storing data that is not useful, and improvements in hardware compression has made packet capture more affordable for enterprises.

Data lakes have become a popular choice to store large amounts of unstructured meta-data generated by networking devices, security tools and IT infrastructure. This meta-data is very useful for threat hunting and a great complement to packet data as it provides a high-level summary of the activity across the network. However, it is only a summary and often lacks specific details required to fully investigate and remediate security incidents. Using meta data in conjunction with packet data can provide this necessary detail.

Storing Packet Data

Storing packet data in a data lake with meta-data is not practical because the volume of data presented for indexing and storage would overwhelm the data lake, resulting in slow queries and rapid consumption of precious resources. A better approach is to enable analysts to quickly pivot from meta data stored in a data lake to the detailed packet data stored in its own repository.

“Collecting and analyzing data from the network will remain a staple of cyber security programs as it provides a foundation for much of the work performed by a security operations center (SOC) and provides the data required for auditing of compliance standards.”

The next question becomes how to store that detailed packet data. One option is to store packet data in a central repository, but this has a few significant challenges. Fault tolerance is the first challenge because if the storage is lost so is all the data. This means centralized storage solutions need to store duplicate copies of the data which is costly. Another challenge is that centralized storage options, such as SAN storage, are typically costly and are not well-optimized for recording packet data.

A better storage option is to use a dedicated, distributed packet storage architecture that allows packet data to be recorded and stored wherever it was originally captured, and for that data to be centrally searchable. This solution minimizes the fault tolerance issue because the loss of a node means only data in that node is lost, minimizing the impact. A distributed architecture also means that network data can be captured and stored locally to the network segment being monitored, thus eliminating the need to retransmit captured network data across the network to a central location. This avoids unnecessary network congestion and removes the need for expensive centralized storage options such as SAN storage.

A dedicated packet capture solution is able to effectively store and index the network data analysts require when investigating incidents while scaling to the complexity and size of modern networks. Integrating packet data into all security tools provides an invaluable common frame of reference. Being able to go from an alert or event in any tool to the related packets makes it much easier to have a reliable view of what actually happened on the network.

Packet Capture Enables Security Analytics

Ideally, datamining and search functionality needs to be centralized to provide meaningful and timely results to teams. Most implementations of packet capture today are included as part of analytics platforms. However, the problem is that when packet capture is treated as a feature rather than a standalone product, the requirements discussed are often not fully met.

Packet capture in these analytics platforms often discards the packet data after it has been analyzed, with the exception of a few packets to show why an alert was triggered. This makes it impossible for security teams to do deep investigations where raw historical data is required. Also, since many analytics platforms have packet capture as a feature, companies end up spending resources on redundant implementations that are unable to share information between each other.

A dedicated packet capture solution allows for higher quality data to be shared to multiple analytics platforms and across multiple teams as required. Security monitoring tools often have a limit to the maximum throughput of traffic they can handle before they start to drop packets. An advantage of a dedicated packet capture solution is the ability to deploy multiple parallel instances of those security monitoring tools and load-balance traffic across them. This allows them, in effect, to be infinitely scalable and prevents the need to replace a solution that starts to exceed its maximum throughput. With the underlying hardware platform in place another instance can simply spin up to handle the load – much like what happens in cloud environments.

Conclusion

A key tenet of any security technology is visibility – you can't analyze data you don't have. A strong, dedicated packet capture solution is the best way to feed high quality data into the security analytics tools teams rely on to do their daily tasks. Adopting a shared common hardware platform approach to providing this packet capture capability has significant benefits—lower cost, increased integration and interoperability between tools that use it, hardware consolidation, reduced management overhead, and greater efficiency for analysts who can access a single, common source-of-truth about what has happened on the network.

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

How Enterprise Security Teams Benefit from Cloud Infrastructure Entitlements Management (CIEM)

Prepared by

Dr. Edward Amoroso
Chief Executive Officer, TAG Cyber LLC
eamoroso@tag-cyber.com

Version 2.0
December 2020

Introduction

The global cyber security community has always benefitted from attention to key foundational principles that help guide enterprise risk management decision making. One of these principles is known as *least privilege* – and it traces its origin all the way back to the earliest days of information security in the 1980s. The principle involves ensuring that privileges are restricted to the absolute minimum required to achieve a given mission objective.

A related security principle involves management of access policies for enterprise applications. Traditionally, an access management function has been used to enforce these policies, but more recently, this function has been managed through so-called *entitlements*. An entitlement provides fine-grained control of who can access what applications under which conditions. When stretched across an enterprise, it creates a new layer of policy control.

As one would expect, with enterprises globally accelerating their adoption of public cloud, a corresponding obligation emerges to perform entitlements management for these virtual assets across multi-cloud or hybrid cloud infrastructure environments. The resulting *Cloud Infrastructure Entitlement Management (CIEM)* is a new control category being promoted across the security industry.¹

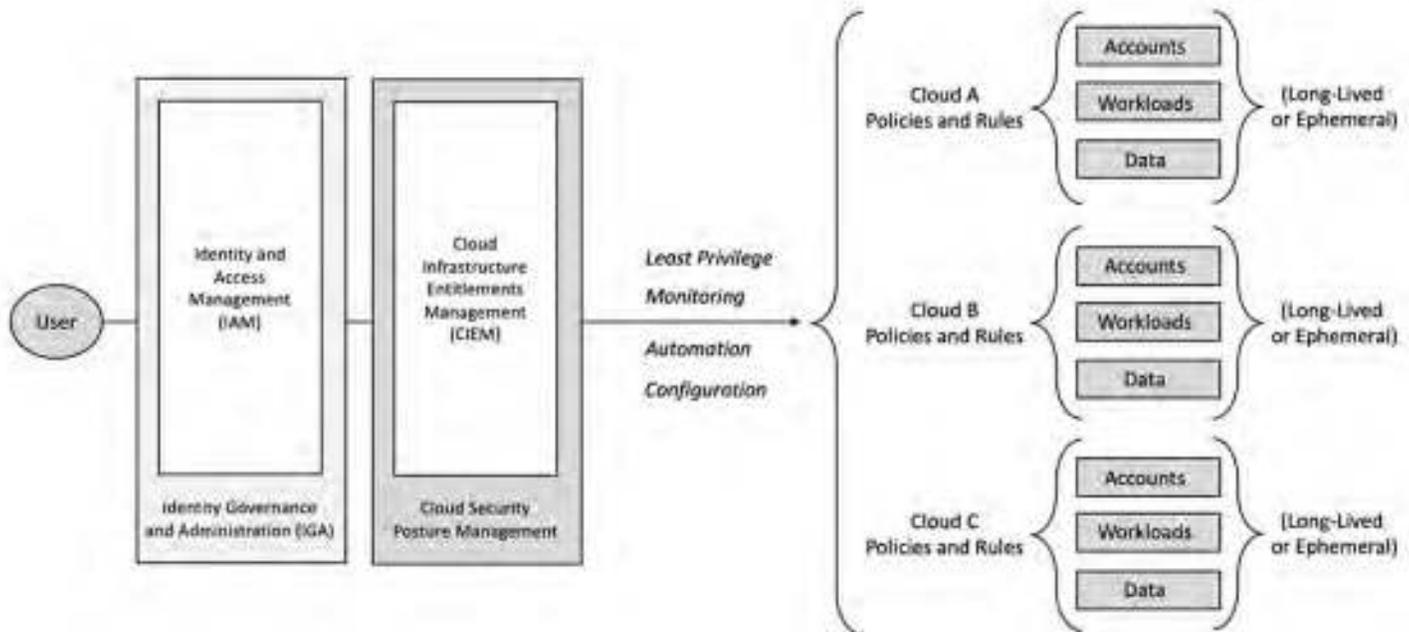
This report provides an overview of how CIEM can be integrated into an existing security architecture, and how it must be coordinated to function with enterprise identity and access management (IAM) protections. The paper also lists the benefits of implementing a proper CIEM platform in an enterprise, with attention to how CIEM fits into the obvious shift for most organizations from on-premises computing to public and hybrid cloud infrastructure use.

Understanding CIEM

For enterprise teams that are guided by their existing legacy security configuration or by familiar protection frameworks such as the NIST Cybersecurity Framework, the concept of implementing a CIEM across their multi-cloud platforms will require a new paradigm and standardizing on a multi-cloud permissions and entitlements management platform. As such, it is imperative that CISO-led teams understand exactly how a CIEM solution integrates with their existing security and identity management tools and how it can be embedded into compliance programs.

Reference to *entitlements* in the context of cloud infrastructure is a minor, but important mindset shift for security teams. By combining elements of authentication and access policies into a common designation, entitlements allow security teams to remove access management from applications and integrate the function into a cloud-based service. This is welcome for teams that want more commonality in policy enforcement across multiple clouds.

¹ <https://www.gartner.com/smarterwithgartner/top-actions-from-gartner-hype-cycle-for-cloud-security-2020/>



Enterprise Benefits of CIEM

With enterprise IT infrastructure shifting toward more virtual, cloud-based operations, security teams are obliged to address the compliance and protection aspects of this change. The good news is that cloud entitlements can be managed with commercial platforms that offer excellent benefit, both for regulatory and compliance activities as well as for day-to-day prevention, detection, and response to cyber threats.

Below we outline five areas of benefit that have emerged for organizations who integrate CIEM platforms into their multi-cloud infrastructure.² These benefits all share the characteristic of reducing overall risk – and each represents an area of cloud security management that is likely to become a requirement in future versions of key security frameworks such as the NIST Cybersecurity Framework (CSF)³.

Entitlement Management – CIEM deployments support rightsizing of entitlements allocations to ensure that permissions are allocated only when needed. Such rightsizing is consistent with least privilege goals for most enterprise permission and privilege schemes. The objective is to ensure that an exact match is provided at all times – including on-demand – for any users, systems, or workloads that require access to some resource.

The extension of enterprise computing to multi-cloud infrastructure makes this a more complex operation. The challenge is that different clouds will have their own policies and rules for accessing accounts, workloads, and data. By augmenting identity and access management with CIEM capabilities, the access management functions for these multi-cloud services can be made more common and uniform across one enterprise.

² Several excellent commercial options are now available for enterprise security teams. The CloudKnox solution team was particularly helpful during the development of this report. They shared deep insights with our analysts into how CIEM platforms work best in the context of a modern hybrid cloud architecture.

³ The existing requirements in familiar security documents such as NIST 800-53 rev. 5 do not yet include reference to the use of CIEM-like functionality in multi-cloud protection architectures.

Credential Risk Reduction – The risk of credential theft or misuse is reduced when entitlements are managed in the context of an authorization model. This is important because so many modern cyber incidents include poor credential management as a root cause. The recent Verizon Data Breach Investigations Report, for example, listed stolen credentials as the number one hacking tactic for the fourth year in a row.⁴

What this means is that CIEM integration into the IAM and multi-cloud infrastructure management not only supports improved posture assessment and compliance, but also will have a meaningful impact on reducing the intensity and frequency of actual cyber attacks. With more enterprise services moving from premise to cloud, this risk reduction should be viewed as an essential step for security teams.

Insider Risk Reduction – Since insiders tend to target user entitlements, CIEM deployments will reduce this risk – especially for cloud infrastructure access. Insiders represent a particularly insidious challenge because they can take advantage of legitimately granted credentials and entitlements. This underscores the damage that can be done when administrators with heavy privileged access go bad.

The use of a CIEM to manage this entitlement allocation process is thus an essential aspect of any preventive cyber defense because it will help avoid the side effects of insiders being granted more access than they actually need. In addition, if a CIEM platform includes on-demand management of entitlements, then it can also help with response actions taken during an attack on cloud resources.

Attack Surface Minimization – By improving management of cloud entitlements, the security team goes a long way toward reducing the attack surface of their organization. Where previously an attack surface roughly matched the corporate perimeter, today's modern attack surface extends out to hybrid multi-cloud infrastructure. This is a major departure from previous schemes and requires a new set of security controls.

As one might expect, CIEM solutions target the primary weakness in this new attack surface extension – namely, the identity and access characteristics of cloud-hosted resources. While it is certainly imperative to include many other types of protections such as activity monitoring and configuration controls, few would argue that properly orchestrating the allocation of entitlements will have a significant impact on reducing risk.

Identity-Related Compliance – Security compliance issues in the modern organization have clearly shifted from local-area systems to sprawling multi-cloud infrastructure. Amidst this change, however, one aspect of the compliance process hasn't changed – and that is the emphasis placed on identity-related issues as a primary control for the enterprise. This has remained a significant focus area despite shifts from premise to cloud.

CIEM platforms are particularly well suited to handle this compliance burden because they can serve as one-stop-shop locations for the types of issues, requests, data requirements, and other obligations imposed by regulators and assessors on the security team. To that end, both security and compliance teams should be involved in the selection of a suitable commercial CIEM solution.

⁴ <https://spycloud.com/a-deep-dive-into-the-verizon-2020-data-breach-investigations-report/>

Next Steps

Enterprise teams who are operating cloud-based services or hosting applications in either private, hybrid, or public infrastructure should immediately begin to review commercial options to manage the entitlements. Luckily, many great commercial CIEM options now exist, so enterprise security portfolio managers should engage to develop requirements for their cloud entitlements management needs.

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

Account Takeover Protection: How to Stop ATO

Account takeover, also known as ATO, is becoming a go-to attack method for cyber criminals based on its efficacy. Armed with legitimate account information, criminals can affect significant damage, to both individuals and enterprises, before the compromised account is detected and disarmed. In this report on ATO protection, we examine why ATO rates have risen and how enterprises can protect themselves and their employees from becoming victims of account takeover.

Prepared by

Katherine Teitler
Senior Lead Analyst, TAG Cyber
katie@tag-cyber.com

Introduction

Account takeover has long been a primary cyber attack tactic. When executed well, cyber criminals gain unfettered access to sensitive resources and data, and trick people—authorized users like employees, partners, and contractors—into giving up further information that allows the attacker to inflict serious damage on consumers and businesses.

As the cyber threat landscape has evolved and businesses have learned how to defend against basic account takeover (ATO), cyber criminals also evolved their tactics to evade detection, now using stealthy bots and impersonation that easily bypass traditional security tooling. However, because compromised accounts can result in significant damage to organizations, businesses must have an ATO prevention and mitigation plan to avoid:

Direct access to funds and other valuables

Account takeover, like other forms of cyber fraud, is a profitable business for cyber bandits. Threat actors use various methods to access users'/consumers' financial accounts, such as bank accounts and crypto wallets, as well as gain access to intellectual property and corporate systems which contain sensitive information. They then sell the stolen information on the black market or develop their own competitive products and services using others' hard work.

Access to sensitive PII or Payment details

One of the most common goals of ATO is gaining illicit access to sensitive personally identifiable information and payment information to sell to third parties on the black market. With this data in hand, criminals are virtually guaranteed profits. In addition, profiteers can use this data to create fraudulent accounts to buy goods and services (without actually paying), exact further scams, spread misinformation, and damage brands.

Brand reputation and revenue damage

Pursuant to the points above, unauthorized access to users' accounts allows cyber criminals to steal information and spread misinformation, which can lead to loss of customers, decreased sales and profits, and the creation of goods and service based on a company's unique designs, thereby rendering them not unique and not as competitive as they should or could be.



Account takeover and fraudulent account creation have far-reaching consequences. They can impact legitimate users via ID fraud and stolen identities, lock users out of their accounts, misrepresent companies and their business practices, steal important and valuable proprietary data, skim payment data, and generally scam good people and honest businesses.

How attackers gain access to compromised credentials

The most prevalent way cyber criminals attempt account takeover is through online scams, such as phishing. Phishing is the #1 way fraudsters trick people out of account information. Phishing is most commonly thought of as targeted email and business email compromise that deceive people into giving up credentials or installing keyloggers and malware that can watch for then steal account information.

However, phishing is a broader problem than email alone. Phishing also constitutes fraudsters setting up fake websites that imitate a legitimate brand, driving web traffic to that site using legitimate SEO techniques recommended by search engines and marketing experts, and then applying common attack tactics, like placing malicious links and phony forms on the website. These methods capture account details, infect the user with malware/ransomware, or install keyloggers that capture user data as unsuspecting website visitors go about their seemingly usual business. Threat actors may also use re-direction, stemming from an infected email, to lure users/consumers to their malicious website.

Mimicked websites often include form fraud, in other words, asking people to enter personal data into a phony form, then cyber criminals use that data to take over the accounts associated with the supplied data. In many cases, because the user does not think there is anything illegal about what is happening, threat actors remain undetected for long periods of time, running up serious financial cost, and ensuring long-term harm against the victims.

In many cases, because the user does not think there is anything illegal about what is happening, threat actors remain undetected for long periods of time, running up serious financial cost, and ensuring long-term harm against the victims.

Malware, such as key loggers that steal credential information or which test credentials for stuffing attacks, are also commonplace for criminals trying to execute account takeover. Criminals may also attempt to use insecure public Wi-Fi to spread malware to connected users, drop malicious files on their devices, and snoop on connections to identify and steal account information.

Point of sale (PoS) systems are another popular way criminals capitalize on legitimate transactions and turn them fraudulent. Software and hard-to-fix firmware vulnerabilities in PoS systems can and have been used to exploit the terminal and its cloud repository to steal payment details as they're entered.

And as with PoS systems, general purpose databases, cloud applications, and cloud storage buckets are attractive to attackers because software vulnerabilities are rampant, patches are often not applied in a timely fashion, and misconfigurations offer access to data and details. These vulnerabilities offer the access threat actors need to takeover accounts, and once the damage is done, even if the vulnerability is patched, businesses and consumers have a hard time stopping the data from being used, especially when only traditional ATO mitigation methods are in place.

How attackers use compromised credentials

In previous sections of this report, we've alluded to how cyber criminals use compromised credentials. Nonetheless, we think the scope of the problem warrants a brief highlight on the consequences of ATO.

The theft of funds from bank accounts or other forms of payment, like mining cryptocurrency and access to pre-paid debit card information, is the primary driver for ATO. Whether criminals are pilfering funds directly from accounts or are making online purchases using stored payment information, money motivates a high proportion of ATO attempts.

In a similar vein, account takeover and unauthorized account access helps criminals steal account credits and rewards points to use themselves or sell on dark web forums to other malevolent individuals.

Identity theft and fraudulent account creation allow criminals to conduct account fraud, such as opening up lines of credit in victims' names, applying for loans, or making big ticket purchases without having to pay for items. Attackers can also open new bank accounts—in victims' names, of course—and use the accounts to launder money. A money mule, or "smurfer," is often hard to track down since their identity is stolen, and the result is years' worth of trouble and anguish for the victim whose name and identity is being used for illegal activities.

Brand and personal-identity impersonation help criminals trick people into all sorts of schemes; from obtaining account credentials and PII that they sell on the black market at premium prices, to business email compromise that installs malware, to setting up phony websites from which they skim account details, impersonation is a major tactic in ATO that helps threat actors inflict damage while staying stealthy.

Measuring the impact of ATO

The costs of account takeover and account compromise—on companies and consumers—is hard to quantify. However, sources estimate that the cost of ATO to businesses is nearly \$7 billion USD in 2021 and grew by over 280% between 2019 and 2020.⁴

Some of these costs are direct costs, meaning, they include the amount of fraud loss, the cost for customer service departments to resolve incidents (time and hourly wages), takedown efforts, lost revenue (money from fraudulent purchases can never be recouped by the provider, nor can the good or services), and the cost of insurance deductibles and increased coverage fees which result from claims against insurance.



Harder to quantify but no less costly are indirect costs that impact companies' bottom lines and consumers' satisfaction. Brand damage and reduced customer engagement are two very important factors that can be harmed by ATO and affect revenue and future viability. In addition, the cost of restoring customers' compromised accounts can total thousands of hours and add significant friction to the business and consumer use.

It is therefore important for businesses to take a proactive approach to stopping ATO rather than waiting until compromised accounts are identified.

Evaluating commercial ATO protection platforms

A commercial ATO prevention solution will allow businesses to identify fake or spoofed sites, identify leaked or stolen credentials and accounts, see when automation is being used to trick employees or consumers into giving up sensitive information, find malicious botnets, uncover automated scripts that chum through passwords and login data, identify malicious IP addresses, and more.

Whatever the method of attack, preventing ATO starts at the source: where credentials are first compromised. Therefore, any viable solution should include the ability to identify the source of data input and stop attackers from propagating an attack.

With fewer account takeover compromises, companies' risk postures improve; their brand remains under their control; employees, customers and partners are better protected; and revenue is not wasted on mitigating threats.

One of the lesser-known aspects of ATO prevention is deception, but it is becoming a capability in some ATO prevention platforms. The idea of deception, when it comes to preventing account compromise, is poisoning data sources—flooding attackers with decoy credentials that seem legitimate and consume attackers' time, or creating fake websites that look like legitimate sites but are populated with fake data to trick attackers. Ultimately these decoy tactics will frustrate attackers when they fail to gain control or when they put up impersonated sites that don't render any harm. Deception allows businesses to create significant noise—in other words, turning the tables on attackers, using their own techniques against them—and making it harder for attackers to takeover accounts and steal data and information.

When evaluating ATO prevention platforms, the following questions will help determine which type of platform your organization needs:

- 1) **Risks** – How is your company currently assessing risk from spoofing, external fraud, and redirection?
 - a. *How are you monitoring external sources for fraud against your company and customers?*
 - b. *Do you prioritize web- and customer-facing web properties as risk factors?*
 - c. *What/where is the greatest risk?*
 - i. *Do you collect personally identifiable information (PII)?*
 - ii. *How is it stored?*
 - iii. *Where is it stored?*
 - d. *What is the business impact if attackers exploit those systems, or use external systems to lure customers into giving up PII?*
 - e. *What is the impact of account creation fraud on your business when a stolen identity is used to make purchases?*
 - f. *What regulatory issues might arise if your business doesn't adequately protect your customer's PII?*

- 2) *Assets – What types of web properties do you maintain?*
 - a. *How many web properties does your company maintain?*
 - b. *How are you tracking updates and changes to your web assets?*
 - c. *How do you identify approved new sites, pages, or applications that collect visitor or customer information?*
 - d. *How are you monitoring for violations against your brand?*

When it comes time to engage with platform providers, it is recommended to incorporate the following criteria:

- 1) *What techniques are used to detect fraud?*
 - a. Machine learning
 - b. Computer vision
 - c. Natural language processing
 - d. Semantic analysis
 - e. Deception

- 2) *What detection features are used?*
 - a. Site similarity/cloning
 - b. Icon and image similarity
 - c. Spoofed login fields
 - d. SSL transparency logs
 - e. DNS monitoring
 - f. Reputational monitoring
 - g. Behavioral monitoring
 - h. Phishing kit detection
 - i. Network and IP data
 - j. User browsing pattern tracking
 - k. Location history
 - l. Device information/hygiene
 - m. Multiple login attempts from disparate devices or locations
 - n. Dark web scanning

- 3) *What types of remediation does the platform provide?*
 - a. Alerts
 - b. Victim tracking
 - c. Blocking
 - d. Takedown
 - e. Forced password resets

- 4) *Deployment*
 - a. How is the platform deployed?
 - b. What architectural changes might be needed to deploy?
 - i. Are any special system permissions required?
 - c. How long does deployment take?
 - d. What system/access rights does the platform require?
 - e. What type of performance impact is expected?

Conclusion

Businesses across every industry rely on their web properties to interact and transact with customers. Threat actors see huge opportunity to exploit customer-facing resources to steal PII, spread misinformation to damage brands, and defraud consumers. What makes this type of attack so complicated to prevent is the fact that threat actors may use external web properties in their impersonations and attack sites; there is nothing on a company's network—on-prem, cloud, hybrid, or otherwise—that can be managed and monitored with network, endpoint, or application technology. Even external scanning tools, those that look for internet accessible for internal resources, are not always reliable since attackers are stealthy and hide their clones.

As the variety and frequency of fraud, phishing, and ATO attacks rise, digital businesses must take a proactive approach to protecting web properties.

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

ⁱ <https://www.darkreading.com/checkers-breach-underscores-continued-pos-dangers/d/d-id/1334852>;
<https://www.zdnet.com/article/wawa-card-breach-may-rank-as-one-of-the-biggest-of-all-times/>

ⁱⁱ <https://www.alluresecurity.com/wp-content/uploads/2021/02/AllureBrochure2021v3.pdf>

DISTINGUISHED VENDORS



DISTINGUISHED VENDORS

2 Q 2 0 2 1

Working with cyber security vendors is our passion. It's what we do every day. Following is a list of the Distinguished Vendors we've worked with this past three months. They are the cream of the crop in their area – and we can vouch for their expertise. While we never create quadrants or waves that rank and sort vendors (which is ridiculous), we are 100% eager to celebrate good technology and solutions when we find them. And the vendors below certainly have met that criteria.



1Kosmos offers next-gen passwordless authentication digital identity proofing with advanced biometrics. The company's innovative approach leverages blockchain, and provides a mobile app experience that allows businesses to verify employee and customer identity without the typical friction or vulnerability of traditional authentication.



Accurics enables self-healing cloud native infrastructure by codifying security throughout the software development lifecycle. The company's products programmatically detect, monitor, and mitigate risks in Infrastructure as Code to reduce customers' attack surfaces and prevent cloud posture drift before infrastructure is provisioned.

Acronis

Acronis Cyber Protect and Cyber Cloud help businesses integrate cyber security, data protection, endpoint management, and backup and recovery to prevent breaches and ransomware. Acronis offers a one agent, one management interface platform, making cyber protection across your infrastructure and endpoints easy and effective.

AGARI

Through applied science, the Agari Identity Graph™ delivers business context to every email risk decision. Agari ensures outbound email from the enterprise cannot be spoofed, increasing deliverability and preserving brand integrity, and protects the workforce from devastating inbound BEC, VEC, spearphishing, and account takeover-based attacks.

TAG CYBER DISTINGUISHED VENDORS

1 Q 2 0 2 1

ATTACKIQ

AttackIQ, the leading vendor of breach and attack simulation solutions, built the first Security Optimization Platform for continuous security control validation. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyber defenses work as expected, aligned with the MITRE ATT&CK framework.



Avanade was founded as a joint venture between Microsoft Corporation and Accenture LLP. The company's solutions include artificial intelligence, business analytics, cloud, application services, digital transformation, modern workplace, security services, technology, and managed services. Avanade helps clients transform business and drive competitive advantage through digital innovation.



Axis Security simply and securely connects users to any application through one centrally managed service. The Axis Application Access Cloud replaces disparate and complicated secure access technologies such as VPNs, VDI and inline cloud access security broker services using a single zero trust platform.



Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with nearly 300 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.



Balbix was founded to help companies to automate cyber security posture and reduce the ever-growing attack surface. The company's BreachControl™ platform uses proprietary algorithms to discover, prioritize, and mitigate unseen risks and vulnerabilities at high velocity, without infinite budgets or large, skilled security teams.



Cloud Range cyber range training allows SOC analysts and incident responders to test and improve attack detection, response, and remediation capabilities within a safe environment. With virtual access or on-site training, users prepare for hyper-realistic attacks against their network and infrastructure and become better defenders.

TAG CYBER DISTINGUISHED VENDORS

1 Q 2 0 2 1

CloudPassage

CloudPassage's Software-as-a-Service product is CloudPassage Halo, a unified cloud security platform that automates security and compliance controls across servers, containers, and IaaS resources in any public, private, hybrid, and multi-cloud environment. Halo's extensive automation capabilities streamline and accelerate.



Constella Intelligence is a leading digital risk provider. Its solutions are powered by a combination of proprietary data, technology, and human expertise—including the largest breach data collection, with over 100 billion attributes and 45 billion curated identity records spanning 125 countries and 53 languages.



Corelight gives defenders unparalleled insight into networks to help protect the world's most critical organizations. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek, the widely-used network security technology.



TAG CYBER DISTINGUISHED VENDORS

1 Q 2 0 2 1



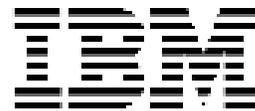
Cybereason is the leader in future-ready attack protection. The company's Defense Platform unifies endpoint protection, security operations, security assessments, and threat hunting to help businesses outthink and outpace attackers. Cybereason is built to interrupt malicious operations, getting customers to mitigation and root cause analysis quicker.



Eclipsium helps organizations manage and protect devices for their distributed workforce, data centers, and networks, down to the firmware and level. The Eclipsium platform provides security capabilities ranging from basic device health and patching at scale to protection from the most persistent and stealthiest threats.



Endace's EndaceProbe Analytics Platform records a 100% accurate record of network activity, while simultaneously hosting third-party network security and performance solutions. The ability to integrate accurate network history into these solutions enables rapid investigation and resolution of network security and performance issues.



IBM Security is one of the largest security providers in the world. IBM's broad security portfolio includes a suite of capabilities across data, endpoints, identity and access, intelligence, and more. IBM security solutions let businesses "put security everywhere" and achieve zero trust across the enterprise.



INKY prevents phishing using a unique method of computer vision and machine learning to stop attacks other email solutions can't see. The company's flagship product, INKY Phish Fence, uses proprietary techniques to block attacks before they reach user inboxes, avoiding costly compromises and financial loss.



Kasada provides the only online traffic integrity solution that accurately detects and defends against bot attacks across web, mobile and API channels. Kasada restores trust in the internet by foiling even the stealthiest cyber threats, from credential abuse to data scraping.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 1



The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps. Netskope understands the cloud and delivers data-centric security, empowering organizations to balance security and speed and reimagine the perimeter.



NowSecure are the experts in mobile app security testing and services. Their platform provides comprehensive mobile app testing for security, compliance, and privacy risk vectors across 3rd party, custom, and business-critical mobile apps, with speed, accuracy, and efficiency.



Okera provides secure data access and governance at scale. The Okera Dynamic Access Platform automatically defines, enforces, and audits data access policies at the fine-grained level using an intuitive zero-code interface. Okera ensures data privacy compliance and that the appropriate data access policies are configured.



Prismo Systems empowers enterprises to transform the way they secure users, assets, and applications with an active risk-based approach. The company's flagship product, the Prismo Transaction Graph, is a data lake purpose-built for security at enterprise scale, providing active cyber risk management.



SCYTHE is an adversary emulation platform for enterprises and cyber security consultants. The company's platform allows red, blue, and purple teams to compile synthetic malware, test defenses against real-world adversarial campaigns, and assess their risk posture and cyber exposure across the enterprise.



Security Risk Advisors (SRA) is a global consulting firm offering advisory services and a 24x7 CyberSOC. SRA's consultants provide specialty services that produce measurable security program improvement. Through a combination of strong technical acumen and strategic insight, SRA serves the Fortune 500 and Global 100.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 1



Semperis provides cyber preparedness, incident response, and disaster recovery solutions for enterprise directory services. Semperis' patented technology for Microsoft Active Directory protects over 40 million identities from cyberattacks, data breaches, and operational errors.



Sepio Systems offers the first hardware access control platform that provides visibility, control, and mitigation to zero trust, insider threat, BYOD, IT, OT, and IoT security programs. Sepio's hardware fingerprinting technology discovers all managed, unmanaged, and hidden devices that are invisible to other security tools.



ShardSecure offers total privacy, zero data sensitivity for data stored in the cloud or in on-prem environments. The company's proprietary Microshard™ technology shreds, mixes, and distributes data to eliminate its value on backend infrastructure, reducing the probability that attackers can exploit or steal sensitive data.



Sirius was founded to improve companies' SaaS deployments by identifying insecure or risky configurations that introduce unnecessary data and access exposure. Focused on the Microsoft Office product suite, Sirius offers quick scans and vulnerability assessments with tailored guidance for organizations' unique business requirements.



Trusona offers true passwordless multi-factor authentication, with a focus on digital identity. Trusona eliminates eight of the most common attack vectors—from credential stuffing to SIM swapping, phishing, and more—and uses biometric authentication and unique visual IDs to confirm users' identities without adding friction.



White Ops is a cybersecurity company that protects enterprises and internet platforms from digital fraud and abuse. The company verifies 10 trillion+ interactions per week, protecting customers' sensitive data, reputation, compliance, bottom line and customer experience as they grow their digital business.

