



TAG Cyber

# Security Annual

3RD QUARTER 2021

A SPECIAL SECTION:

# THE INZ MODEL

IDENTITY  
AUTHENTICATION  
AUTHORIZATION

ARTICLES / OPINIONS / INTERVIEWS

### WELCOME TO THE 2021 TAG CYBER SECURITY ANNUAL – 3RD QUARTER EDITION

**A**s we kick off the last half of 2021, the world is once again looking at a “new normal.” The abundant social, political, and health changes over the last year plus have been more than enough for everyone, but cyber security practitioners have had the added challenge of securing highly fluctuating workforces and onboarding myriad device types on a consistent basis. As workforces now begin to think about moving back into offices – at least in part – and fire up business travel, security teams must incorporate many of the lessons learned since the start of the pandemic and adjust to hybrid environments that accept more flexibility and personal device-driven connectivity than ever before.

To be sure, many organizations were well on their way to hybrid operating environments pre-pandemic, but it’s fair to say that now *most* organizations will retain a portion of what they had to accept during it. The push to allow remote connectivity, from anywhere, at any time, from any device regardless of its security hygiene was a daunting task that tired security teams had to accomplish.

Now, as public places open up, organizations have determined that in-office requirements will be significantly reduced and use of corporate-owned devices will no longer be mandated. These policies could not be possible without the lightning-fast shift to cloud. While cloud migration and adoption were already well on their way (with an **estimated 94% of companies at least some form of cloud at the start of 2021**), the tech world had never seen an increase in volume and speed like it did at the start of 2021. With more systems, services, and access to sensitive data hosted in the cloud, new security challenges exist for data protection, identity management, and access control.

Indeed, we at TAG Cyber have seen such an uptick in interest around next-gen identity and access management solutions that we split authentication from its traditional housing under IAM and gave it its own place in our new taxonomy.

Speaking of, you will see a very big change in how TAG Cyber categorizes its research. In the next section, read about how and why we’ve migrated away from the 54 controls to a set of 26 tier one categories with over 130 subcategories. Yes, cyber security is *that* big and complicated! Nonetheless, we feel our new taxonomy – albeit bigger – is simpler for enterprises evaluating technology and the vendors building it.

The new taxonomy also helps us introduce our new research subscription. This service allows enterprises to research the technology market, learn about trends, find best practices, and shore up their programs as they fight against the ever-growing cyber crime syndicate and malicious hackers.

Whatever the end of the year holds, we can be certain that cyber crime won’t decrease. In the last months since the publication of the 2021 Second Quarterly, the number of attacks against U.S. critical infrastructure has been astonishing and demoralizing, highlighting the need for enterprises to focus on foundational cyber hygiene and implement zero trust-based, multi-layered approaches to data, network, enterprise and endpoint security while tightening up governance and enforcement (our nod to the legacy 54 controls).

Unfortunately, but realistically, many enterprises have failed to take the necessary steps to prevent, detect, and stop attacks. Though a “shift left” approach to cyber security is commendable, it is prudent to simultaneously take a “shift right” approach; it is without a doubt that cyber adversaries will continue



to be successful in penetrating defenses. The challenge now is reducing mean time to detection and mean time to remediation. It is absolutely unacceptable to **shut down a fuel pipeline** for over a week and cause a national scare because backup controls weren't in place to compensate for ransomware that initiated at the endpoint.

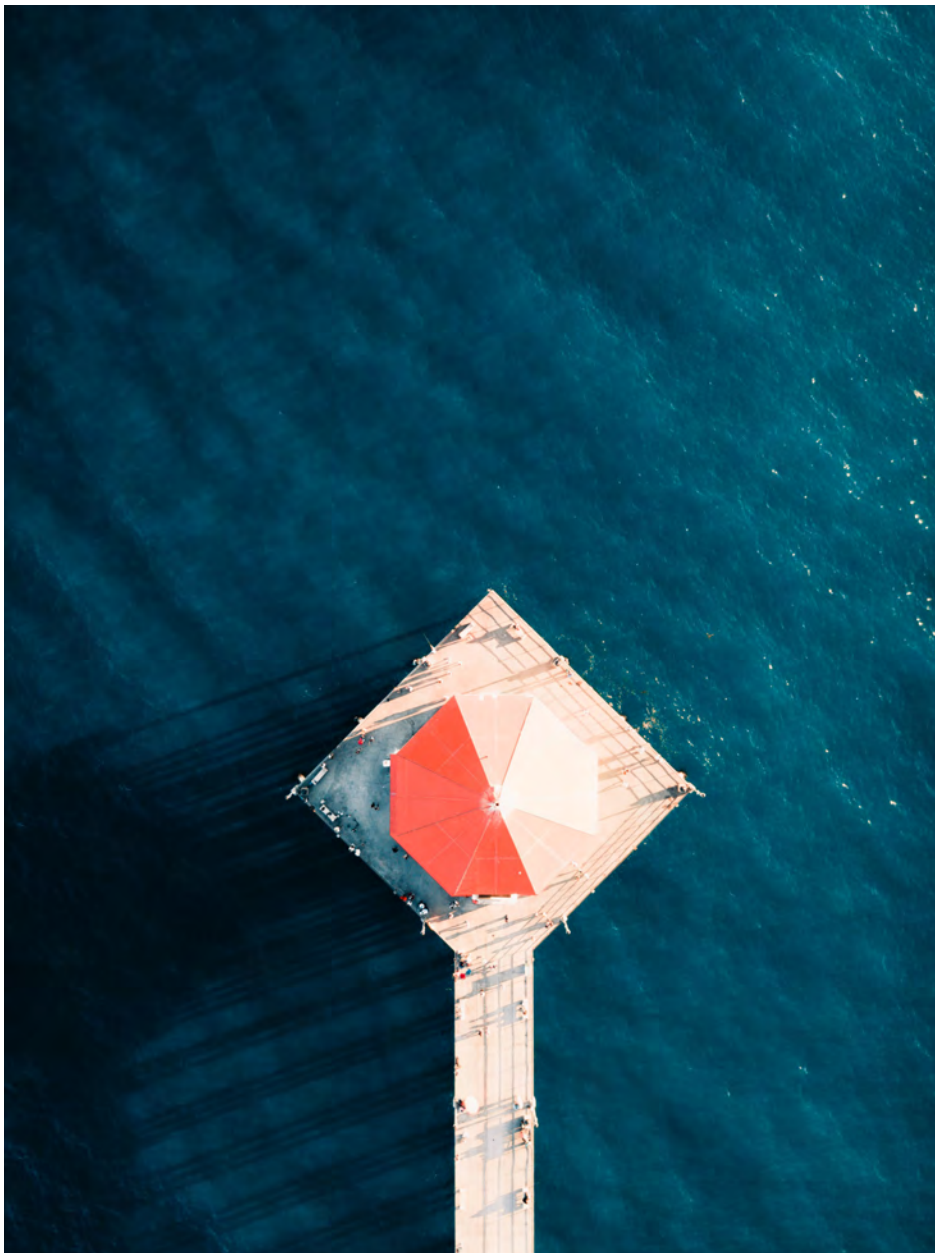
Similar ransomware attacks, including those on **JBS**, New York's **MTA**, Massachusetts' **MBTA**, several hospital systems, **Fujifilm**, **Bose**, and more highlight why security teams are searching for processes and technologies to harden systems and prevent the propagation of an attack. Regardless of its intrusion point.

The White House, too, has been quick to step in, issuing an **executive order** aimed at protecting the nation's private businesses and critical infrastructure. While we at TAG Cyber believe the order does **not go far enough**, it is a start. And we hope to help companies of all sizes and across all industries advance their security programs. This is our mission at TAG, and whether you just read this Quarterly, call us to talk through your cyber program and purchases, or subscribe to our research, we want to be part of the solution. We know we all have a long way to go, but 2021 is only half over!

Thanks for reading our Q3 report. As always, we hope you learn something and are inspired to try something new to substantively improve your cyber program today.



*"Which one is AWS?"*



FEATURED DRONE PHOTOGRAPHY:  
UNSLPASH, SHUTTERSTOCK

- **LEAD AUTHORS** – Ed Amoroso, Katie Teitler
- **RESEARCH AND CONTENT** – Adam LeWinter, 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.**

July 15, 2021



Introduction	2	Reduce your MTTD and MTTR with Cyber Range Training	
Overview of the TAG Cyber Taxonomy (FKA: Controls) for 2021	5	Debbie Gordon, Cloud Range	64
<b>THE INZ MODEL</b>	<b>10</b>	Model "Good," Normal Behavior to Prevent Phishing and Business Email Compromise	
Introducing the INZ Model for Identity, Authentication, and Authorization	11	Crane Hassold, Agari	67
From What's Your Password to Why Have One?	16	Using Compromise Intelligence to Prevent Cyber Attack	
Managing Identity Without Having an Identity Crisis	19	Karim Hijazi, Prevaillon	69
<b>OP-ED</b>	<b>24</b>	Continuous Assessment and Control for Cyber Risk Management	
Cyber Security vs. Cybersecurity	25	Anjan Venkatramani, Prismo Systems	72
Managing Misconfigurations to Stop a Data Breach	28	Creating a Secure, Confidential Cloud Computing Environment	
Biden's Executive Order Will Not Stop Cyber Attacks	30	Ayal Yogev, Anjuna	75
We Need More Science in Cyber Security	32	Protecting High-Value Workload from Cyber Compromise	
Have Your Friends Asked You About Blockchain and Cryptocurrency?	36	Dave Furneaux, Virsec	78
<b>INTERVIEWS</b>	<b>38</b>	Defending the Modern Corporate IT Infrastructure with XDR	
Protect Your Network with DNS Data		Sam Curry, Cybereason	81
David Ratner, HYAS	39	Innovation to Spur Delivery of Unified Application Protection	
Convenience, Privacy, and Security with Passwordless Authentication		Sean Leach, Fastly	84
Michael Cichon, IKosmos	42	Proactive Attack Surface Management for Risk Reduction	
Securing Critical Infrastructure via Observability		Brian Hazzard, Randori	87
Josh Lospinoso, Shift5	45	<b>ANALYST REPORTS</b>	<b>91</b>
Can You Quantify Your Insider Data Risk?		Using Self-Healing to Achieve DevSecOps	92
Tommy Todd, Code42	48	Automation as the Kill Switch to Malicious Bot Attacks	96
Elevated Email Threats? Not with Human Layer Security		Toward Secure Business Networking 2.0	104
Tony Pepper, Egress Software	50	Take Back Control of your Hybrid Work Environment	109
Learn from Your Data to Improve Detection and Response		Securing Emerging 5G Global Network and Mobile Infrastructure	117
Leon Ward, ThreatQuotient	53	What Every CISO Should Know About Insider Threats: An FAQ and Security Checklist for CISOs	125
Rendering Data at Rest Incomplete and Unintelligible to Threat Actors		Investigating Data-Centric Security Strategies	132
Jesper Tohmo and Zack Link, ShardSecure	56	<b>DISTINGUISHED VENDORS</b>	<b>136</b>
A Forensic Approach to Ransomware Prevention			
Anthony Di Bello and Raj Munusamy, OpenText	60		



# OVERVIEW OF THE TAG CYBER TAXONOMY (FKA: CONTROLS) FOR 2021

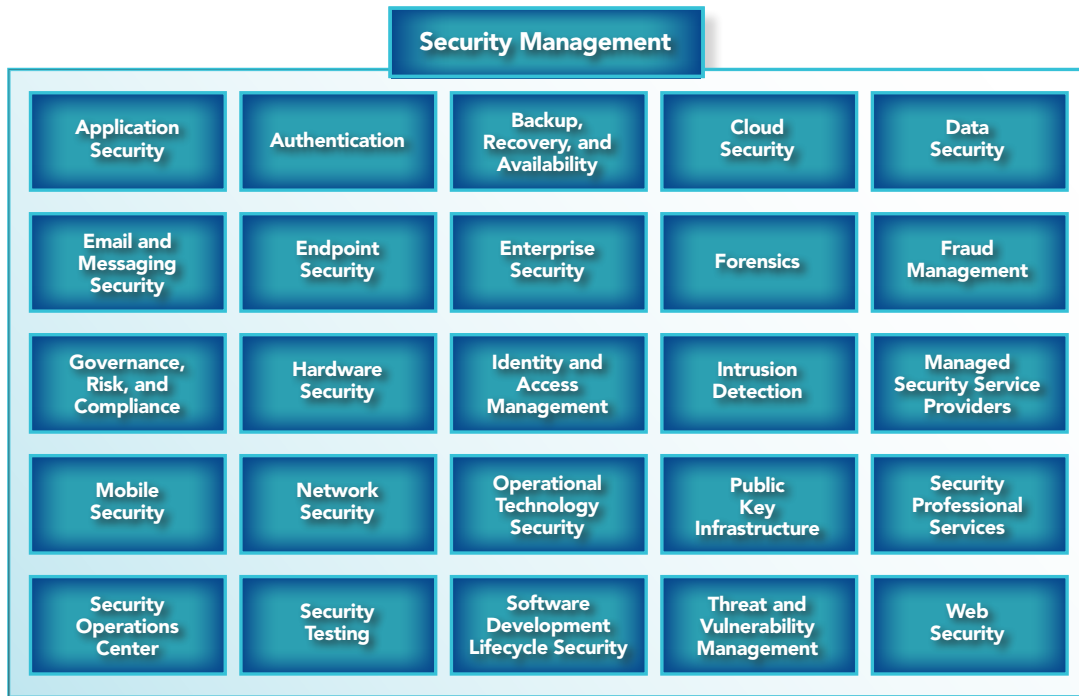
## INTRODUCING THE NEW TAG TAXONOMY

Those who know TAG Cyber know that the company was not founded with a pitch book but with a mission statement: *to democratize world-class cyber security industry research*. A first step in that direction was to provide the cyber security professional community with practical advice on how to comprehend and grapple with the vast maze of cyber security products and services. There is still no doubt that Lego-like building blocks with studs for controls, vendors, and products are a cyber security community exigency, as well as a requisite for sensible research. Yet the security landscape is complex and our efforts to create a catalog did not fully realize the goal of transparency into the landscape. We thus set a goal for 2021 to publish a holistic description of cyber security that nonetheless provides full visibility into all its nooks and crannies.

Updating our taxonomy was both a labor of love and a challenge, the biggest of which was avoiding the temptation to simply create yet another cyber security framework or standards document. Our goal in this endeavor was and is helping enterprises navigate the ever-growing complexity of the cyber security landscape—not tell them how to do it. The purpose of our new taxonomy is to define how to **decide** what controls you need and how to **manage** the controls you have. It is our hope you will think of the taxonomy as describing what you need to run your security program, not how to do it as defined by any one-size-fits-all categorization.

Our recognition that controls are just a piece of the puzzle should in no way be interpreted as disrespect for the concept of controls. TAG's mission to democratize world-class cyber security industry research and analysis began with a set of six cyber security control categories: *Enterprise, Governance, Network, Data, Endpoint, and Industry*. We supplemented them with fifty well-defined subcategories in the form of security product and service descriptions. The concept served our clients well for the first five years of our journey and was used to compare and contrast CISO requirements and strategies. We thought of it as a cubbyhole approach to storing our analysis in a way that could be easily retrieved. But tangible control definitions are as often overly broad as they can be narrow. In the original TAG categories, concepts underlying the control definitions protruded out from under different categories in different directions. We concluded that it is more important to organize our thoughts with respect to these concepts than to fully describe any one product or service, because the concepts help us and our clients arrive at correct visualizations of any cyber security product or service.





## TAG Taxonomy – Level One

Thus, TAG Cyber recently landed on a **taxonomy** rather than another revised control set. Our taxonomy aims to be flexible and adaptable to accommodate the rapid pace of change in cyber security and offers mechanisms to monitor and adjust for change as needed. We also appreciate that, by adopting a taxonomy, we aligned with those in physical sciences, and with that comes a scientific approach to classifying cyber security taxa.

## THE TAXONOMY

As in any taxonomy, the “taxa” attributes determine placement. Teams of experts can identify new attributes and place them in an existing node **or** evolve the taxonomy itself. The taxonomy is not a list of controls, but a classification system for controls. Just as the hierarchy in biology from *Domain*, *Kingdom*, on down to *Genus* and *Species* helps biologists understand animals, the TAG Taxonomy helps us understand cyber security products and services. It is a job aid for research, to help us to think clearly about control attributes and compare and contrast cyber security product and service features. This structure is an acknowledgement that cyber security has attributes in common with any management discipline, and that category can be thought of as the source of use cases for the remaining 25.<sup>1</sup>

## COMPARE/CONTRAST

Cyber security standards communities mostly agree on process, on “how” cyber security should be managed, not on the “what”. No specific technologies are universally applicable and recommended. The hesitancy to declare “what” is universally sanctioned is because, like an accountant who needs to use judgement to recommend whether capital set-aside reserve is sufficient to cover market risk and credit risk, a cyber security professional is constantly badgered to align controls with business

<sup>1</sup> For those of you familiar with the ACM Computing Classification System, also a job aid for research, yes we did explore it but found it too narrowly focused on computer science to serve a practical professional attempting to navigate the cyber security marketplace.

## TAG Taxonomy – Level Two

### Security Management

- Board Communications
- Budgeting
- Business Alignment
- Certifications and Training
- Leadership skills
- Personal Productivity
- Policies and Strategy
- Recruiting, Hiring, Retention
- Team Management

### Application Security

- Application Programming Interface Security
- Container and Kubernetes Security
- Dynamic Application Security Testing
- Interactive Application Security Testing
- Mobile Application Security Testing
- Runtime Application Self Protection
- Software Compositional Analysis
- Static Application Security Testing

### Authentication

- Biometrics
- Passwordless Authentication
- Password Management
- Mobile Push
- MultiFactor Authentication

### Backup, Recovery, and Availability

- Business Continuity/ Disaster Recovery
- Cloud Backup
- Data Center Backup
- Infrastructure and Directory Resilience
- Ransomware Prevention

### Cloud Security

- Cloud Access Security Broker
- Cloud Data Encryption
- Cloud Security Compliance
- Cloud Visibility
- Cloud Workload Protection
- Public Cloud Security
- Multi-Cloud Security

### Data Security

- Data Classification
- Data Discovery
- Data Encryption
- Data Inventory Management
- Data Leakage Protection
- Digital Rights Management

- Gateway Data Leakage Protection
- Privacy Platforms
- Quantum Cryptography
- Voice Encryption
- Secrets Management
- Database Security

### Email and Messaging Security

- Anti-Phishing
- Domain-Based Message Authentication, Reporting, and Conformance
- Email Encryption
- Secure Email Gateway

### Endpoint Security

- Antivirus Software
- Browser Isolation
- Content Disarm and Reconstruction
- Endpoint Detection and Response
- File Integrity Management
- Internet of Things (IoT) Security

### Enterprise Security

- Asset Management
- Business Application Security
- Directory Security
- Database Security
- Enterprise Asset Inventory
- Physical Security
- Rules Management
- Secure Collaboration
- Secure File Sharing
- Operating System Security

### Forensics

- Cloud Forensics
- Digital Forensics
- eDiscovery
- Law Enforcement Support
- Mobile Forensics

### Fraud Management

- Account Take-Over Detection
- Anti-Fraud Analytics
- eCommerce Fraud Protection
- Web Fraud Prevention

### Governance, Risk, and Compliance

- Automated Compliance Support
- Compliance and Regulatory Support
- Cyber Insurance
- Risk Management Services
- SaaS Compliance Services
- Security Metrics

### Hardware Security

- Firmware
- Hardware Security Modules

### Identity and Access Management

- Authorization
- Cloud Infrastructure
- Entitlement Management
- Consumer Identity and Access Management
- Identity Governance and Administration
- Identity Services
- Privileged Access Management

### Intrusion Detection

- Attack Surface Protection
- Deception Security
- Intrusion Detection System
- Intrusion Prevention System
- User Behavioral Analytics

### Managed Security Service Providers

- Extended Detection and Response
- Government Information Assurance
- Managed Detection and Response

### Mobile Security

- Mobile App Security
- Mobile Device Management
- Mobile Device Security
- Mobility Infrastructure Security

### Network Security

- Cloud Firewalls
- Domain Name System Security
- Distributed Denial of Service Security
- Network Access Control
- Network Detection and Response
- Network Monitoring
- Next-Generation Firewalls
- Secure Access Service Edge
- Secure Remote Access
- Software Defined Wide Area Network
- Virtual Firewalls
- Virtual Private Network Services
- Zero Trust Network Access

### Operational Technology Security

- Industrial Control System Visibility
- Industrial Control System Mitigation
- Supervisory Control and Data Acquisition Security

- Unidirectional Gateways
- Vehicle Security

### Public Key Infrastructure

- Certification Authority
- Cryptographic Lifecycle Security
- Secure Sockets Layer Support

### Security Professional Services

- Security Assessment
- Security Awareness and Training
- Security Coaching
- Security Industry Research and Advisory
- Security Research
- Security Strategy
- Value Added Resellers
- Virtual CISO

### Security Operations Center

- Incident Response Support
- Log Management
- Security Information and Event Management
- Security Orchestration, Automation, and Response
- SOC as a Service
- SOC Automation
- SOC Simulation Range Training
- Threat Hunting Tools

### Security Testing

- Automated Penetration Testing
- Breach and Attack Simulation
- Bug Bounty / Crowdsourced Security Testing
- Penetration Testing
- Blue/Red/Purple Team

### Software Development Lifecycle Security

- DevOps Security
- Infrastructure-as-Code Security
- Software Process Maturity

### Threat and Vulnerability Management

- Digital Risk Protection
- Patch Management
- Security Scanning
- Security Scoring
- Third-Party Security
- Threat Intelligence
- Threat Sharing Support

### Web Security

- Bot Management
- Content Security
- Secure Web Gateway
- Web Application Firewall
- Web Proxy
- Website Scanning

requirements to reduce cyber security risk to an acceptable level. This level varies widely from company to company and is based on numerous factors – not one set of standards that can be applied broadly to different and disparate organizations.

Further, while accountants have had over 5,000 years to come up with Generally Accepted Accounting Principles (GAAP), cyber security professionals have had less than a century to decide what controls could be used to manage cyber security risk – and there are certainly a bevy of excellent technologies (“what”) on the market to accomplish cyber risk reduction. Our taxonomy, therefore, is a helpful aid in the classification of the plethora of vendor solutions constantly coming down the pike; it is intended to facilitate one’s ability to perform classifications accurately and thereby coax assessments toward correct conclusions. To a driver, the taxonomy is more of a GPS than a steering mechanism for a gap analysis.



### SUMMARY

The TAG Cyber mission statement remains intact: *to democratize world-class cyber security industry research*. The new TAG Taxonomy is expected to provide clarity and transparency on complex cyber security systems and processes for practitioners, students, researchers, and industry analysts from a wide variety of fields.

As the industry constantly evolves, TAG Cyber, too, must evolve and change. For now, our new classification system is all that changes — and we believe it is more accurate and comprehensive than before. What does not change with this new classification system is our mission and our passion for improving the cyber security industry. We thank you for coming along on our journey thus far and look forward to many discussions with you about the industry, our taxonomy, and how the field of cyber security must continue to change and evolve.







A SPECIAL SECTION

# THE INZ MODEL



## INTRODUCING THE INZ MODEL FOR *IDENTITY, AUTHENTICATION, AND AUTHORIZATION*

EDWARD AMOROSO

*Existing cyber security models like SASE were not designed to address higher-level protection requirements for users and applications. The INZ Model\* is introduced here to complement network security models and to help complete the emerging enterprise security picture.*

### MOTIVATION FOR INZ MODEL

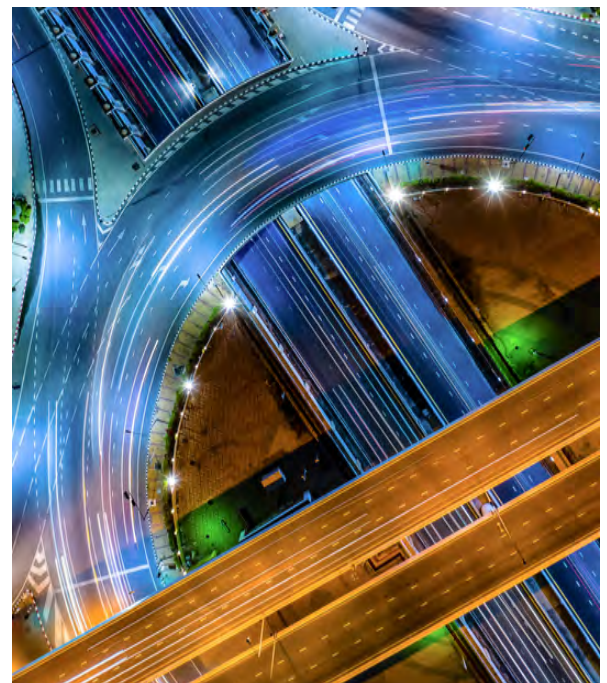
Cyber security practitioners use models to guide their protection efforts. This started with the Bell LaPadula<sup>i</sup> and Biba<sup>ii</sup> models, which helped early IT managers determine the best means for labeling sensitive data to avoid confidentiality and integrity problems. It continued with the Clark-Wilson<sup>iii</sup> model which helped early security professionals design schemes to maintain the validity of assets.

Recently, the SASE Model (Secure Access Service Edge) has had considerable influence in the security community. It provides an accurate view of how cloud-based controls are beginning to drive enterprise network security design, thus resulting in a new distributed edge. SD-WAN, next-generation firewall, cloud access security, data leakage protection, and other features are enabled via SASE across a virtualized network.

A challenge, however, is that many observers have begun to view the SASE model as the definitive model for enterprise security – and while this is fine for the underlying network, it is insufficient to cover critical user-level controls. Specifically, it leaves out how users and entities are authenticated, how workflow authorization is managed, and perhaps most importantly, how identities are managed and validated.

In this paper, we introduce a simple model called INZ (**I**ntity, **A**uthen**ti**cation, and **A**uthor**iz**ation), which we

The problem is that enterprise IAM never sufficiently covered cloud use cases and left out many important dependencies such as with authorization policy.



*\*The design of INZ was assisted greatly through discussions with Mark Clancy, CEO of Authority.*



believe offers a useful guide to complement SASE in these additional user and entity-level aspects of enterprise security. It is designed to serve as a basic checklist for how each function is to be implemented individually, but it also serves to guide the respective interactions and dependencies that exist between each element of the model.

## INZ MODEL OVERVIEW

The simplest abstract representation of INZ depicts the three elements as a triangle from which we can derive the most important interactions and dependencies. We do not see any one point on the triangle as being more or less important than any other. Identity, authentication (authN), and authorization (authZ) are each empowered in the context of support from the other two elements of the INZ model.

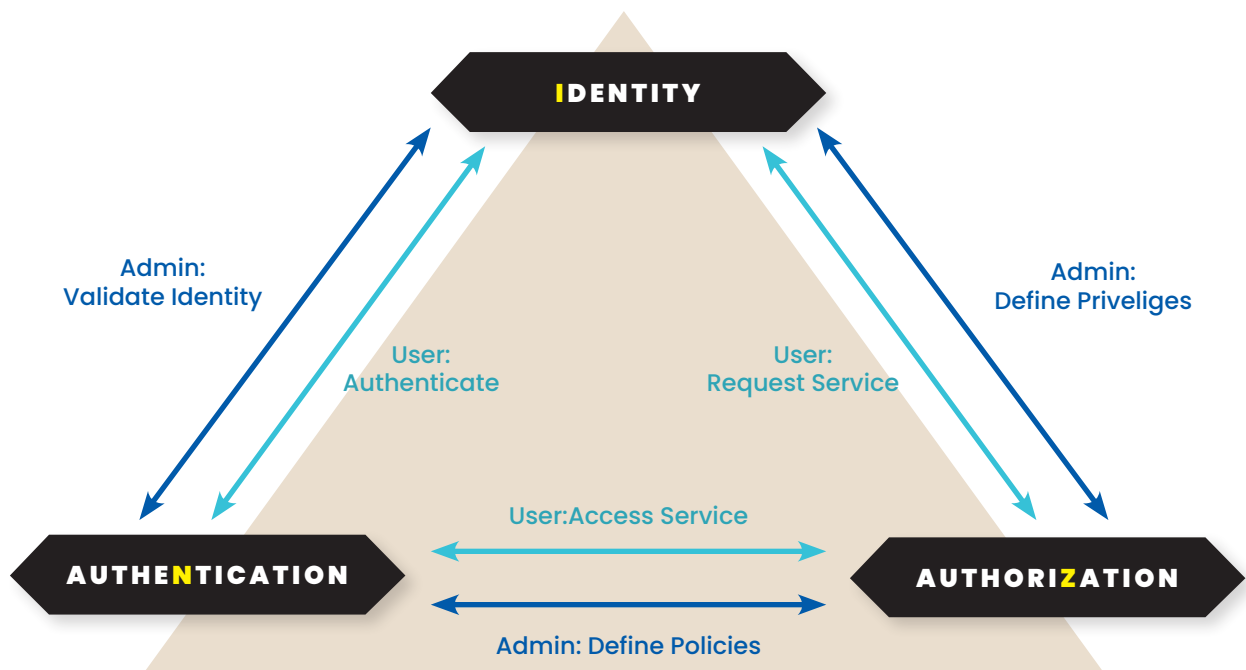


Figure 1. INZ Model

The elements of the model are straightforward and help to depict the types of requirements that must be addressed in the new enterprise. It is influenced heavily by existing identity and access management (IAM) solutions which provide a basis for most existing deployment. The problem is that enterprise IAM never sufficiently covered cloud use cases and left out many important dependencies such as authorization policy.

## IDENTITY CONTROLS AND DEPENDENCIES

The model starts with the obligation every enterprise has to determine their local definition of what constitutes an *identity*. This might seem obvious in a typical corporation where users consist of employees and contractors, but in more complex environments, such as service providers, identities can correspond to individuals, billing addresses, device identifiers, digital identifiers, and so on.

While each local environment will establish the specific identity-related functions that must be managed, the TAG Cyber analyst team has observed several activities in many of the best enterprise security designs.

These identity-related functions are listed below, not as a complete checklist, but as representative examples of the types of identity control that must be considered by enterprise security teams:

- **Identity Proofing** – This involves the means by which identity claims are made, presented, and verified, often by a third-party identity provider (IdP).
- **KYC Onboarding** – The acronym KYC (know your customer) references the processes required to identify and verify the identity of customers.
- **Digital Wallet** – This mechanism is commonly used to securely store and connect payment information to an individual.
- **Federated SSO** – This is the means by which SSO (single sign-on) is implemented based on identity that is federated (securely shared) by an authoritative source.

## AUTHENTICATION CONTROLS AND DEPENDENCIES

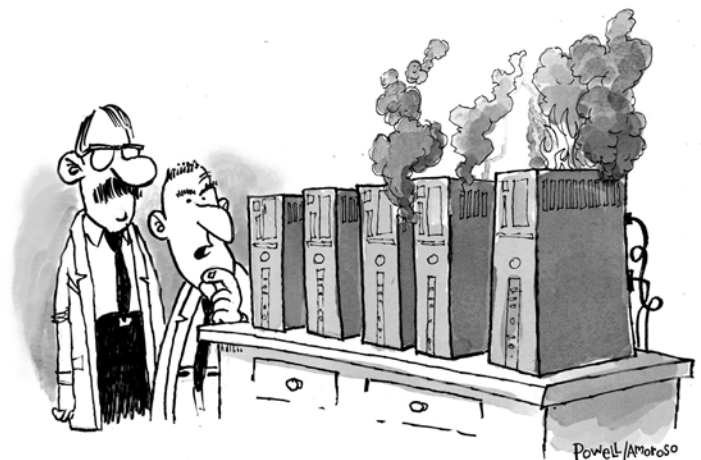
The INZ model continues with authentication – and this should come as no surprise to any observer. Many major cyber security incidents in the past decade, including the famous attack on Colonial Pipeline, have included some sort of deficiency in how authentication is handled. Amazingly, many enterprise teams continue to rely on stored passwords, often citing (erroneously) that complex password requirements are sufficient.

As was the case for identity in the section above, the list of representative authentication-related controls shown below does not constitute a complete checklist of what must be done in this area. The authentication requirements will differ between organizations, especially in ones that include industrial controls, which increasingly must utilize machine-to-machine validation solutions, often based on cryptographic support.

- **MFA** – This is the common means by which multi-factor authentication (MFA) is used to validate reported identities.
- **Workload Authentication** – Workloads require authentication, which implies some mechanized service authentication, often using cryptographic methods.
- **Passwordless Experience** – This involves the common goal to remove passwords from the user experience, often through standard such as FIDO (Fast IDentity Online).
- **Biometrics** – Biometrics involve the use of personal characteristics such as fingerprints and facial patterns to validate a reported identity.

## AUTHORIZATION CONTROLS AND DEPENDENCIES

The final aspect of the INZ model involves the obligation of every enterprise to develop a working means to support authorization policies. Typically, authorization is driven by business needs to enforce policies based on privileges,



*"I guess a couple of our systems didn't like the MITRE ATT&CK testing."*

rights, and other user-level attributes. Workflow approval processes are perhaps the most familiar aspect of authorization implementations that readers will recognize.

As in the previous two sections, the list of authorization functions for enterprise that are listed below includes some representative capabilities each enterprise must implement. Unlike identity and authentication, these functions tend to include business process and application leaders more heavily. These functions also have had to adjust to workload support in emerging hybrid and public cloud architectures.

- **User Privileges** – This involves assignment and management of privileges that match an individual’s or group’s work requirements.
- **Granularity of Rights** – This is the process of defining and assigning sufficiently granular access and usage rights to business functions.
- **Application Policy Enforcement** – This involves management and enforcement of access policies for business applications.
- **Cloud Policy Enforcement** – This involves management and enforcement of access policies for cloud-hosted applications.

**The end goal of the INZ model is to complement existing models such as SASE toward a more comprehensive view of how the enterprise is protected both at the network level and at the user/application level.**

## INZ DEPENDENCY CYCLES

The INZ model depicts two dependency cycles – one that focuses on user-initiated activities (the inner circle in the model) and another that focuses on administrator-initiated activities (the outer circle in the model). In the sections below, we outline the salient aspects of these two dependency cycles with emphasis on how practitioners should create realistic means to cover the requirements in the model.

### USER DEPENDENCY CYCLE

The user dependency cycle in the INZ model includes the respective connections, sharing, cooperation, process support, and coordinated activity that exists at the user and application level between the respective identity, authentication, and authorization functions. These dependencies include bi-directional interactions, and the most important aspects are outlined briefly in the list below.

- **Authentication** – This dependency involves users presenting identity information to be validated as part of the authentication process.
- **Request Access** – This dependency involves the validation of any identity data to mediate an access request for a given service.
- **Access Service** – This involves the granting or denial of a requested access to a service by a requesting individual.



## ADMINISTRATOR DEPENDENCY CYCLE

The administrator dependency cycle in the INZ model includes the respective connections, sharing, cooperation, process support, and coordinated activity that exists at the administrator and manager levels between the respective identity, authentication, and authorization functions. As with the user dependency cycle above, these dependencies include bi-directional interactions, and the most important aspects are outlined briefly in the list below.

- **Validate Identity** – This dependency involves the presentation, validation, and use of identity-related information.
- **Define Privileges** – This dependency involves definition of privileges to be used in access to business resources.
- **Define Entitlements** – This dependency involves definition of the access policies that govern access to business resources.

## ACTION PLAN

Enterprise security teams are advised to use the INZ model as an overall checklist to ensure that they have covered the appropriate identity, authentication, and authorization functions. This is best done by:

1. addressing each element in the model (points in the triangle) with a clearly stated set of policies, and then,
2. addressing each bi-directional dependency (curved lines in the model) also with clearly stated policies.

The end goal of the INZ model is to complement existing models such as SASE toward a more comprehensive view of how the enterprise is protected both at the network level and at the user/application level. Such coverage will help to reduce cyber risk for practitioners and introduces a more complete set of control requirements to be used by enterprise auditors, security assessors, and other stakeholders in enterprise protection.

<sup>i</sup> [bit.ly/3wGF9WD](https://bit.ly/3wGF9WD)

<sup>ii</sup> [bit.ly/3xtXKVL](https://bit.ly/3xtXKVL)

<sup>iii</sup> [bit.ly/3cQOh2V](https://bit.ly/3cQOh2V)

# FROM WHAT'S YOUR PASSWORD TO WHY HAVE ONE?

DAVID HECHLER



Matt Stamper

I first learned the art of asking questions in a classroom, when I was an English teacher. I'm not sure if Matt Stamper has done any formal teaching. Stamper is the chief information security officer at EVOTEK, a consultancy that helps businesses shift from traditional IT to multi-cloud computing. But he is also the co-author of the ["CISO Desk Reference Guide"](#), so I'm sure he's packing

at least an inner teacher. And based on two long conversations we've had, I bet he has more than that. He seems to relish wide-ranging discussions.

I gave him a homework assignment before our recent talk. I asked him to read "Decoupling Identity and Authentication: Introducing the INZ Model," by Ed Amoroso. But the first question I tossed him was a bit of a curveball. I didn't ask it to trip him up (I knew it wouldn't). I wanted to encourage him to explore our subject without feeling constrained by Ed's article, or anything else.

Whenever I email my financial adviser with an order to buy or sell an asset, I told Stamper, he requires me to repeat my instructions over the phone. Is that phone call an authentication or an authorization?

"It's both, if you think about it," he said. Stamper quickly added that it would be important for my adviser to verify that he's speaking to the "authentic David" and not someone trying to spoof me. A minute later he asked if I remembered ["Quadrophenia,"](#) the 1975 film based on the rock opera by The Who.

We were off and running. I hadn't seen the movie. An important theme was "we have very bipolar lives," Stamper said. "We have personalized our professional lives. Multiple personalities end up showing up in these applications." That's where Stamper's view of the movie's

"Having multiple ways, almost an infinite number of ways that we can validate the identity of an individual is going to be the new norm. It has to be."



message intersected with Amoroso's article about decoupling what he calls INZ: **I**ntity, **A**uthen**t**ication, and **A**uthor**iz**ation.

We covered a lot of ground over the next hour. We talked about the simplest method some hospitals use to authorize the amputation of a leg: marking it with a Sharpie. (Stamper later sent me an article that **proved** even this method isn't foolproof.) We talked about the importance of employee training and a book called "**The Checklist Manifesto**", by surgeon Atul Gawande. The book focuses on the importance of hospital procedures, but it also extols the preflight checks that pilots use and credits this approach for **Chesley Sullenberger's** ability to land a commercial airplane in the Hudson River.

Eventually we settled into a more direct discussion of the topics at hand, including the subject that has a tendency to puncture optimistic predictions of a brighter future: passwords.

## THE AUTHENTICATION SMORGASBORD

There are lots of ways to authenticate identity these days. Stamper enumerated some. Biometrics allow a company to use a fingerprint, a voice, a face. Multifactor authentication can pair passwords with answers to security questions, or with codes users receive on authenticator apps and then type into a box. But none of these guarantee security, he added. Deep fakes can mimic some biometrics, notably voice. Data centers that store biometrics can be compromised and the data manipulated.

The same technology that protects security can be unleashed in ways designed to do harm. "Having multiple ways, almost an infinite number of ways that we can validate the identity of an individual," Stamper said, "is going to be the new norm. It has to be." Legacy approaches are no longer working. "The way we're handling authentication today," he continued, "based on the number of data breaches, spoofed identities, Identity theft and the like, is fundamentally failing. We're in this watershed moment. We do have to rethink this."

That's where decoupling comes in. Decoupling components, Stamper said, is "a logical extension of what we're seeing elsewhere. Modern architectures are fundamentally very modular. You can assemble things a little bit here, a little bit there. Bring them together and you've got an application."

## CREDENTIAL MANAGEMENT AND IDENTITY GOVERNANCE

INZ is "one half of a coin," he continued. The other side is "broader credential management, broader entitlements." The identity infrastructure needs to help a company manage least-privilege and need-to-know access. And separation of duties. When auditors are examining a publicly traded company running SAP, Oracle, or one of the Microsoft Dynamics ERP packages, Stamper said, "you're looking at the levels of permissions, rights, and entitlements by an individual user." The quintessential issue in finances, for instance, is: "Does somebody with receivables rights have payable rights as well?" he said. "Because if they do, they can effectively create a nice little closed loop and pay themselves."




*"How about this one ...uh, open-minded couple seeks healthy, middle-aged pair for free sharing of Splunk logs and security best practices."*



Identity governance has grown more important during the pandemic because remote workforces often leave personal and professional lives commingled. And that can create problems for companies. Stamper threw out an example. “You’re my boss, and you’re going to fire me,” he said. “And you think I live in five systems or applications within our company. But the reality is I’m in 10 others that weren’t discovered. And so I get marched out the door, but I still have access to these other systems—or I might have remote access.” That’s what makes how we think about credentials, and entitlements, and authorizations so complicated. And so important, he added.

**“There’s this notion that everything is going to flow into the cloud. But it isn’t.”**



## THE PROBLEM WITH PASSWORDS

As we began to talk about legacy authentication, we came to the inevitable subject of passwords. What makes them such a problem, Stamper said, is that cracking a few often gives criminals access to a dozen or more of a user’s accounts, since passwords are so often reused—and multifactor authentication hasn’t been as widely adopted as one might think.

Where does that leave us? I asked. Does he see a passwordless future? Can they be completely replaced by biometrics?

This was where our earlier talk about “infinite ways to authenticate” met a finite reality. It’s not that easy, Stamper said. It’s analogous to the way some people view cloud computing, he explained. “There’s this notion that everything is going to flow into the cloud. But it isn’t.” A lot of data remains on premises, in traditional data centers. “When we look at how we authenticate and manage credentials, we’re going to have a variety of environments. It will be as hybrid as anything else that’s out there.”

You can replace passwords with superior authentication systems like biometrics, he said, but not all. Some legacy systems don’t allow approaches other than usernames and passwords. Not all systems are **SAML**-compliant or support modern authentication technologies. We can avoid creating them in the future, he noted. Companies can make the old systems a little more secure, he added. But some can’t be retooled and can’t be dropped: “I don’t think we’ll ever see the day when passwords are completely gone.”



AN INTERVIEW WITH JEANETTE MANFRA AND  
BERT KAMINSKI, GOOGLE CLOUD



## MANAGING IDENTITY WITHOUT HAVING AN IDENTITY CRISIS

Cyber security officials working in the White House were actively plotting a murder. The intended target? Passwords. Those pesky vermin that authenticate user identities. Jeanette Manfra revealed the high-level plot during our recent interview. Manfra is a director of risk and compliance at Google Cloud. Earlier in her career she worked as assistant secretary for cyber security and communications at the U.S. Department of Homeland Security. Prior to that she was on the National Security Council staff at the White House. We invited her to talk about *Identity, authentication, and authorization*, which we're calling INZ for short, and the challenges they pose to building security. We also invited her colleague Bert Kaminski to join her. Kaminski, an in-house lawyer and director at Google Cloud, previously worked at Oracle. They had lots to say about how their company is toiling to improve security—for employees and customers alike—without introducing improvements that feel like work. And we did have a little fun with passwords, the security headache everyone loves to hate.

**TAG Cyber:** *When you think about identity, authentication, and authorization, what are the biggest challenges to strengthening security?*

**JEANETTE MANFRA:** Similar to most security areas, there are technological challenges. There are also significant cultural and operational challenges. And the way that many organizations think about these three is built off of decades of evolution. Thinking about how we improve identity management, both from a technological and an operational standpoint, can be very challenging. The current methods are deeply embedded into how organizations operate—for providers and users. If we want to change that, we have to provide alternatives that cause less friction, because introducing more friction into the equation is not going to increase adoption. And then we have to think about how to change habits.

**BERT KAMINSKI:** This has become a big issue recently because of the vast increase of spear phishing. Some of that is driven by the ability of scammers and cyber criminals to scan the web, find identifiers of users, and then convert that into unauthorized access. Credentials are being compromised, passwords are being stolen, and users are being tricked by social engineering into giving up some of their authenticators. So this is the challenge to security.

**TAG Cyber:** *It's almost impossible to have a conversation like this without talking about passwords. Are they doomed? Can they be completely eliminated? And is that your fondest wish? I mean, have you ever considered ways to murder the password?*

**MANFRA:** When I was still in the government, I

**“We haven’t had a single phishing incident related to a password compromise since the introduction of the security keys.”**  
– Jeanette Manfra

was on the National Security Council and working for the White House cyber security coordinator, and he would always say, “How are we going to kill the password dead?” And this was several years ago. There have been a lot of efforts. It gets back to the technology, and operations, and the culture. The password started in a much simpler environment. And it made sense at the time. And then, as hackers got increasingly sophisticated, we said, “Let’s just make it more complicated.” To the point where you’ve got like this 26 alphanumeric, crazy thing that you can’t possibly remember. And then if you do remember, you just use it for every single service that you have, which of course undermines the whole purpose. I think we can live in a passwordless future. I think many people—from businesses to our grandparents—would love to be able to live in that future. Google has done a lot to try to get us there, as have many other organizations. In the last couple of months we’ve talked about how we’re going to be automatically enrolling all of our users into two-step verification. Thinking about other things, whether those are biometrics or phones, there’s a lot of things that can be used in place of a password. I do think it’s going to take us a long time. The concept of a very complex password is here probably for a while. I use Chrome Password Manager personally. It suggests a complicated password, I don’t even remember what it is, but it’s automatically logged into my password manager and stored there.

**KAMINSKI:** Passwords will probably be phased out, but before that they will be increasingly strong and increasingly encrypted. I’m just taking a look at the recent [executive order](#) that was issued earlier [in May]. And there’s a section that mandates that the federal government implement stronger cyber security standards, which includes, among other things, multifactor authentication and encryption. So passwords being stored in an encrypted manner is going to be needed. But the whole point of a password is to identify a user in the system. And you’ll never end up having a situation of completely decoupling authentication and identity. You need to have some sense of who is in the system, are they the right people, and are they in the right areas and doing the right things?

***TAG Cyber: Let’s jump to the pandemic and the fully remote workforces that we’ve been living with for quite a while now. How has that affected all of these security issues?***

**KAMINSKI:** Certainly the pandemic has caused a rapid move of work from home. The Bring Your Own Device (BYOD), work from anywhere at all times was a huge trend, of course, before that, but the pandemic really accelerated the process dramatically. McKinsey was estimating it would take a company around 22 months to implement the full work from home. And actually companies have pivoted into it in about 11 days. But that creates the challenge of multiple devices and multiple time zones





accessing from all sorts of different endpoints at all sorts of times. So you're no longer within the confines of a corporate firewall, knowing who's in and who's out. When you have this heterogeneous way of accessing, it's much harder to ensure that you've got the right users. Companies have been adopting a zero trust approach toward security, which essentially means that you assume that everyone who's trying to enter is an attacker. That really has made the challenge of identity and access controls that much more prominent.

**MANFRA:** We're a pioneer in what is now called zero trust. We refer to it as Beyond Corp, which literally means beyond the corporate network. Zero trust can be confusing, because it's come to mean a lot of different things. But at Google, there was a key security insight before I got here. The location of your network doesn't provide you with any intrinsic benefits anymore. There was this notion of having a digital fortress, and everything inside is something or someone you can trust. But that corporate network doesn't give you inherent trust anymore. In addition to that security insight, maintaining productivity with a decentralized workforce and without the use of a VPN was also an important goal for Beyond Corp. Zero trust is strongly linked to identity, by the way. You have to ensure you have the correct mechanisms in place to appropriately authorize and authenticate individuals and assets. Many organizations were thinking about zero trust or had already begun implementing it when the pandemic forced them to jump full body into it. And in many ways, because organizations were struggling to manage the VPN capacity they needed to have all of these users log in, they were trying to quickly figure out how to take legacy security and apply it to their full workforce. And they had no idea where everyone was connecting from. That's why we saw a lot of people trying to take a multiyear zero trust digital transformation and cram it into a couple of months.

**TAG Cyber:** *As we think about this INZ issue in security, there's the workforce and the internal implications for a company. And there's also how you're dealing with your customers, your clients, your consumers. Do you see them as a separate set of challenges?*

**MANFRA:** At Google, everything we make available externally was first used internally. We're trying to eat our own dog food—figure things out, try to work out the kinks before we release it. The products that Bert and I are using internally are the same that we have or will soon externalize to others. For example, the identity authorization mechanisms and security tokens that we use internally are capabilities now that we offer through our Advanced Protection Program to all customers. Coming from my last organization in the government, where we were really just

**“Privacy law recognizes security as being a key element. And this is why it’s called ‘data protection.’ You can’t have privacy without the security element.”**

**– Bert Kaminski**

starting on our journey to the cloud, to an organization that has all of these zero trust capabilities built in—it’s an amazing experience. We haven’t had a single phishing incident related to a password compromise since the introduction of the security keys.

**KAMINSKI:** There’s one difference when it comes to identifying users who are consumers versus employees. Putting Google aside, for external users like consumers, a lot of companies validate identity through personal information, such as birthdays and social security numbers. You don’t necessarily need to do that when it’s an employee. You have different kinds of credentials and IDs to validate an internal user, versus external consumers. Other companies tend to sometimes pick up and utilize personal information more than you would for an employee.

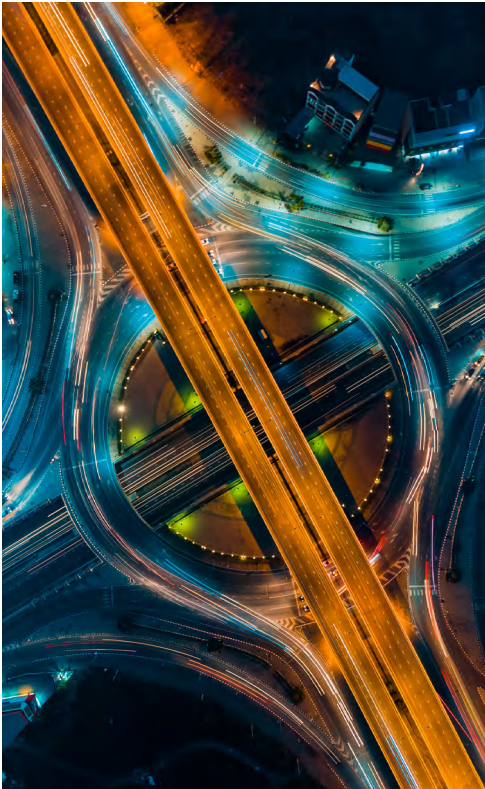
**TAG Cyber:** *And I would assume that you’re less worried about friction internally. I mean, it’s part of your job, right? If you have to go through a little friction, fine. But you don’t want to lose customers.*

**MANFRA:** There’s significantly less friction here than I was previously used to. But as an organization, you have to calibrate. If you have highly sensitive information, then you’re going to introduce more friction, and your users need to accept that if they want to work on this highly sensitive information. What I like about the way that Google has approached it, and other organizations as well, is we recognize that if we make it too hard, nobody’s going to do it. There was a great analogy that I heard once. When thinking about people signing up for retirement plans, if you provide people an opt-in model, you get very low acceptance rates. But once organizations started automatically signing up new employees, suddenly you’re getting 80, 90%. And you do the same thing with security. We need to make security automatic and invisible to the majority of people.

**KAMINSKI:** I’ll just add that it’s all about trust. Users may be willing to take the extra steps if they trust the system and the service. When you’re talking about a market-facing solution, people will utilize your service and buy your products if they feel that they’re secure. And they may be more willing to do that if you show that it’s a benefit as opposed to a burden.

**TAG Cyber:** *Are there ways in which recent improvements in security have collided with requirements or desires for privacy? I note that Google is headquartered in California, and California privacy laws are changing rapidly and have taken the lead in this country, which doesn’t have a federal privacy law.*

**MANFRA:** I see security and privacy as largely two sides of the same coin. The more security you can build in the system, usually the more privacy you are also building into the system. There are



times, as you noted, where either through practice or through the way the tech works, you need information that some may consider private in order to achieve security outcomes. What's interesting about what's happening right now is the search for a definition of what is private information. And if you compare the U.S. versus Europe, there's a rich debate. You need to get specificity in order to be able to implement it on the technical side. Which specific types of data are personal or private? Should a user have a right to some privacy? And what's the difference between a consumer versus an employee of a company—and how the company needs to be able to implement certain security measures? How much privacy should I expect as an employee?

I don't have perfect answers to all of these. A lot of what we're working on internally is, again, how can you have the best security while having the necessary guarantees of privacy? But as to the definition of what privacy means, you noted that there's not a federal privacy law. There's a patchwork to the extent that some states have it, and it usually deals with breach notification and things like that. You also have evolving concepts in Europe and beyond. But I do believe that it can collide, oftentimes when it comes into forensics. And when you want to be able to say, "OK, is the subject of the email private?" That's very useful for doing forensic analysis on spear phishing emails. Is an IP address private? That's very useful for security configuration. To me it's about defining and getting to a consensus on what a user and/or employee should have as a reasonable expectation of privacy. And then how do you realign our security practices and tooling to account for that?

**KAMINSKI:** There's not necessarily a trade-off. Privacy law recognizes security as being a key element. And this is why it's called "data protection." You can't have privacy without the security element. Google is very committed to tracking these laws and providing security and privacy built into its products and services. That's fundamental to the DNA of what Google does. We want the best user experience not only from a performance standpoint, but from a trust standpoint as well. So we engineer privacy and security in it. And the data protection laws require that. Some are more prescriptive than others. As you know, there are certain state laws that actually talk about encryption, and others speak more about using reasonable security based on the circumstances and type of data. One last point. Although a California company, Google works to adhere to privacy laws that apply both in California and elsewhere.





OP-ED



# CYBER SECURITY VS. CYBERSECURITY

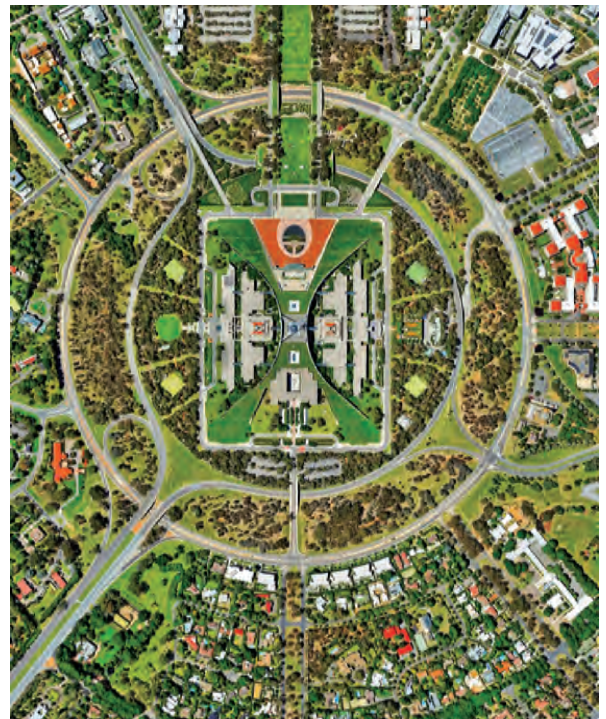
KATIE TEITLER AND JENNIFER BAYUK

*The debate between “cybersecurity,” one word, versus “cyber security,” two words, remains one of the industry’s most controversial topics, to semi-quote one of TAG Cyber’s clients who recently questioned our two-word version. To reinforce his seriousness on the topic, he added a smiley face to his emailed comment, tacitly agreeing that it should not be of tremendous significance. Yet while many practitioners in the field are comfortable with either version, some have very strong feelings about the proper and correct representation of where “cyber” lands in relation to “security.”*

Those of us who have lived through the transitions from computer security to information security to cyber may be more comfortable with the two-word version because it aligns with the adjective form with which other “security” realms are modified: physical security, password security, email security, network security, cloud security, data security, etc. etc. etc. When “cyber” first became a thing, its usage followed a similar convention (though admittedly the accepted written form has evolved in some circles): cyber insurance, cyber forensics, cyber threat, cyber attack.

For the record, most major dictionaries and style guides have since adopted “cybersecurity,” one word, as a noun. However, several reputable industry entities—media sites, trade journals, and vendors—still have “cyber security” published as a two-word phrase. Also, there are a plethora of others which switch back and forth. For example, the **SANS** tagline is: “The most trusted source for cyber security training, certification, and research” but right underneath the tagline on its website, it prompts visitors to “Learn In-Demand Cybersecurity Skills from World-Leading Instructors.” A similar switch is observed in the **U.S. Cyber Command**—two words—declaration that cyberspace (one word) is a domain in which there are cyberattacks (one word).

**If the world’s “leading” instructors and institutions flipflop between usage, the average person would be forgiven for also playing fast and loose with the spelling and/or choosing one and sticking to it for no other reason than preference.**





Source: [SANS.org](https://www.sans.org)



Source: [cybercom.mil](https://www.cybercom.mil)

Why has “cybersecurity” caught the attention of grammarians while other cyber fields remain modestly in adjective mode, for example, “cyber insurance”? Why have terms like “cyber attack,” “cyber threat,” and “cyber criminal” evolved to one-word conventions. No one has been able to provide a real answer.

Now, back to our observations and usage: Thus far, no one has truly pressed TAG on the issue because it just hasn’t mattered that much. Surely no one is going to quibble about whether someone writes “cyber security” or “cybersecurity.” If the world’s “leading” instructors and institutions flipflop between usage, the average person would be forgiven for also playing fast and loose with the spelling and/or choosing one and sticking to it for no other reason than preference.

So...blog over?

Not so fast. The topic has recently surfaced with both new TAG Cyber employees and our **Distinguished Vendors**. Roughly half of our clients assume typo when we write “cyber security,” and new employees often default to “cybersecurity” in their initial writings. When we explain that our style guide dictates the two-word version, no one quibbles. But the repeated suggested edits speak for themselves.

It’s important to note that it has only been in the past 10 years or so that security professionals (see how easy it is to sidestep the issue) have accepted the “cyber” label at all. For many years, stalwarts insisted that it was silly to start calling themselves “cyber” practitioners when “information security” covered it.

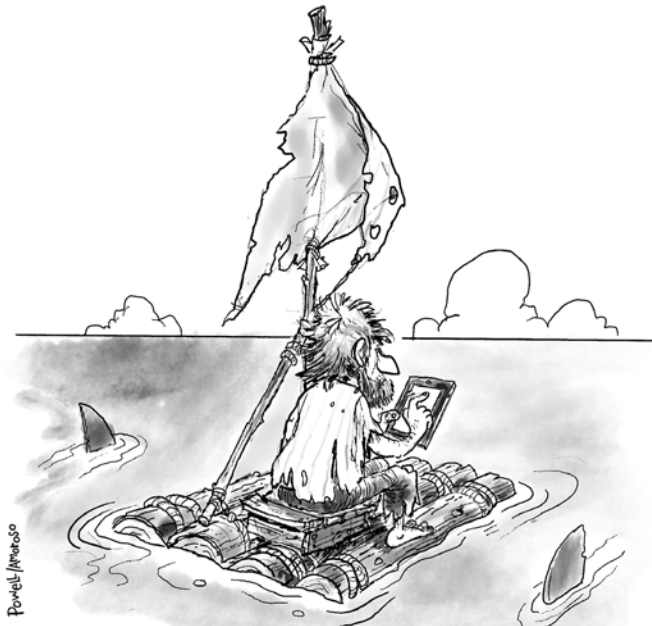
But as “cyber” caught on, both in vendor marketing materials and in the press, the security community started to let go of hostilities toward the new naming convention. Why? Probably because 1) a naming convention wasn’t the biggest problem security pros had to tackle and 2) reasonable arguments could be made that cyber security refers to not just securing the data, information, and systems/technologies that house data and information (i.e., “information security”), but adds the caveat that the data/information/systems are internet-connected in an ecosystem that includes people, processes, and policies governing acceptable use. Thus, “information security” fell out of favor to describe the discipline and “cybersecurity/cyber security” became de rigueur.

Meanwhile, the people heading the world’s leading security programs were and continue to be called “chief information security officers” or “chief security offers,” no cyber in sight.

With these anecdotes in mind, the question becomes: Does it matter how we write cyber security/cybersecurity? Is it just a silly distraction that keeps getting brought up because it’s fun and insignificant? Or does this really make difference in our space, as in, how the rest of the world views information security/cyber/cybersecurity. Does one standard naming convention help us raise the bar?

We truly have not seen enterprise security programs getting derailed over how to write the term. Thank goodness. Then again, people and companies do take the time to agree on their accepted version.

We hope this blog post is not the most important thing you’ve read today, but we do hope you will let us know what you think about “cybersecurity” vs. “cyber security” and why. Maybe you’ll even influence how TAG Cyber refers to the discipline in the future.



*"June 8. Still no Wi-Fi."*



# MANAGING MISCONFIGURATIONS TO STOP A DATA BREACH

KATIE TEITLER

Vulnerability management is a mainstay of most cyber security programs. It is seen as essential by enterprise teams, but rarely do defenders get excited about finding and applying a missing patch or tightening up access controls to critical systems. Sure, it feels good to know you've plugged a hole that needs plugging, but all the glory goes to the threat hunters and even the red teamers who first get to exploit and then fix (or at least tell others how to fix) a vulnerability.

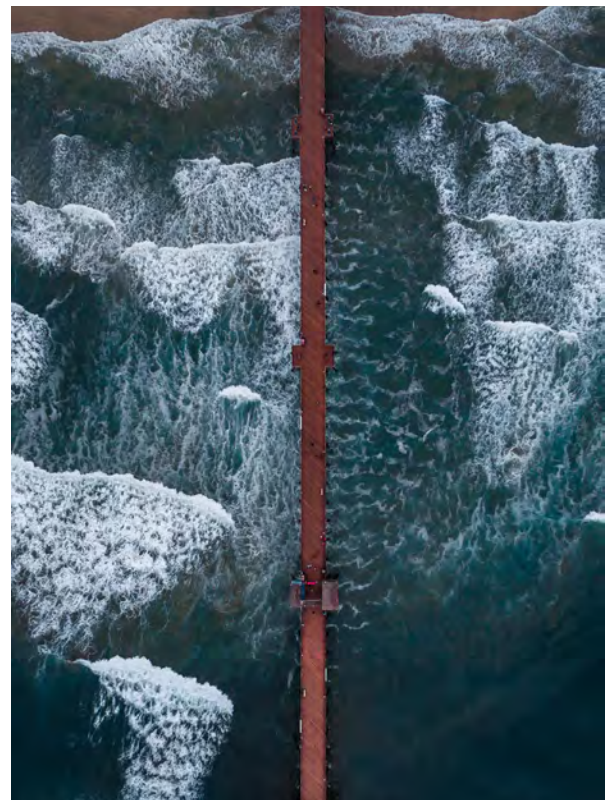
Nonetheless, enterprises would be in a much worse state than they are without sturdy vulnerability management programs. Bubbling to the top of the list of remediation activities for these important teams (which may be an amalgamation of system admins, database admins, cloud architects, security staff, and other asset owners), is configuration management. According to a [2020 survey of 300 CISOs](#), conducted by IDC, 67% of CISOs said that security misconfiguration is a top concern associated with cloud production environments. The [2020 Verizon Data Breach Investigations Report](#) shows that misconfigurations are likewise a top contributing factor to data breaches, increasing as the facilitating factor in data breaches since 2015, and rising 4.9% since the 2019 DBIR—the highest one-year jump for any of the action varieties listed. Of those misconfigurations, a full 21% were due to error rather than malicious intention. What's more, [a study by McAfee](#) estimates that 99% of cloud misconfigurations go unnoticed.

There are many more statistics to be found about the state of the problem, but let's focus on what companies can do to drive down misconfigurations and (likely) breaches that could result from an exploit of one of those vulnerabilities in companies' cloud environments.

## VIE FOR VISIBILITY

One of the main causes of cloud misconfiguration is lack of visibility. Given the ephemerality and distribution

**Traditional vulnerability scanning may not identify misconfigurations because the scanning is not trained on the right resources or the scan is not continuous.**



of cloud instances, vulnerability management teams are challenged to identify default settings that need security's attention. Traditional vulnerability scanning may not identify misconfigurations because the scanning is not trained on the right resources or the scan is not continuous, thus not accounting for new resources spinning up and down.

Cloud-native security scanning and asset management tooling can help. Not all solutions are created equal; ensure that the tool of choice doesn't require vulnerability management teams to poke holes in firewalls to conduct an identification process, thus creating another vulnerability for the organization.

## CARETAKE YOUR CREDENTIALS

Needless to say, compromised or weak credentials pose a major threat to unauthorized access. A threat actor posing as a legitimate user gives unfettered access (especially if accounts are overprovisioned—see below) to the cloud environment and its sensitive or proprietary data and information.

To prevent compromised or weak credentials from becoming the vulnerability your organization doesn't need, enable multifactor authentication for all IAM users and deploy a tool that can discover and remediate unused security groups

## POLISH UP PERMISSIONS

In the same vein as auditing cloud assets to identify risky settings, user and service account permissions must be a focus for cloud vulnerability management. Excessive permissions easily go unnoticed because the defaults for new resources and services are almost always too much. Threat actors can leverage excessive privileges within a compromised node to access an adjacent node and find insecure applications and databases. The result: a destructive data breach with potential compliance consequences.

To remediate this vulnerability, make certain access permissions are reviewed regularly, that least privilege access is applied by default, and that no instance is publicly accessible (which is surprisingly common).

## ENSURE ENCRYPTION

Encryption is one of the easiest ways to prevent unauthorized individuals from seeing what data reside in companies' systems. For instance, enabling S3 bucket encryption will protect the bucket and all new objects stored in it (for data at rest and data in transit). That said, even though it's called "default encryption," the setting is, ironically, not enabled by default. It is trivial for users to configure the setting, though. Be mindful, however, of existing objects at the time of encryption. Objects stored in the bucket prior to flipping the switch on the setting must also be encrypted. In S3, this can be accomplished via Batch Operations.

For every cloud environment, users/admins must review encryption settings to make sure the data is properly protected through its lifecycle. Encryption can be client side or server side—or both. Not all cloud providers' environments are the same, though, so understand the "default" settings for each provider and what "default" means, then take appropriate action.

## CONCLUSION

At present, cloud misconfigurations present a high data breach risk. The reasons for this are myriad: lack of visibility, misunderstanding of "default" settings, inaccessibility of settings, not enough expertise to manage configurations, time and resource constraints, and more. However, fixing misconfigurations is manageable via cloud-native vulnerability technologies. From discoverability to policy enforcement, tools and techniques are available to help organizations understand and control their security posture.

# BIDEN'S EXECUTIVE ORDER WILL NOT STOP CYBER ATTACKS

EDWARD AMOROSO

On May 12, 2021, President Joseph Biden signed the [“Executive Order on Improving the Nation’s Cybersecurity.”](#) I believe the order is well intentioned and was developed by industry experts – many of whom I’ve personally known for years. But the order is just too long and includes far too many unattainable goals. Sadly, I believe the order will come and go – and we will continue to see an uninterrupted series of cyber attacks on our nation’s infrastructure. Below are my top five concerns about the order:

## CONCERN 1: THREAT SHARING

For the past several decades, since [Richard Clarke](#) introduced the idea to our community, there has been a misconception that sharing of threat information will ease cyber risk. I see no evidence that this is true. The order starts with a narrative about removing barriers to threat sharing that could have been written in 1995. It will make no more difference now than it did when we tried this route then. (Read [PDD63](#) from 1998 and compare to the present order.)

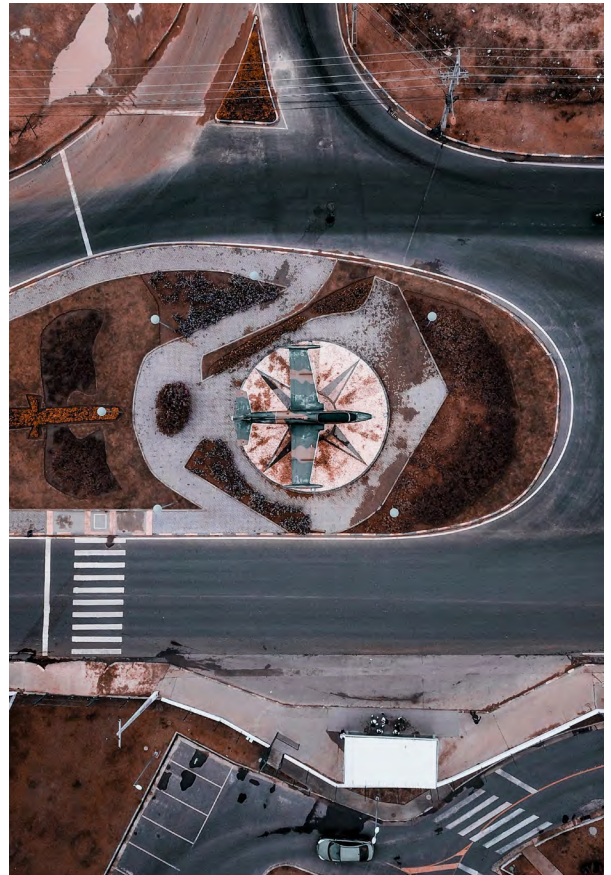
## CONCERN 2: REPORTING CYBER INCIDENTS

For the past several decades, the government has been promoting the idea that reporting of cyber incidents will improve our nation’s ability to prevent attacks in the future. I see no evidence that this is true. The order goes into much detail about driving this forward and I think the process is irrelevant. Rather than shame organizations into fixing problems to avoid reporting, it instead drives reporting-fatigue as more and more incidents are detailed.

## CONCERN 3: SIXTY DAY PLANS FOR AGENCIES TO ZERO TRUST

While I applaud the boldness of demanding that agencies provide sixty-day plans to [zero trust](#), I suspect that this will be an unattainable goal for most. Does the

Rather than shame organizations into fixing problems to avoid reporting, it instead drives reporting-fatigue as more and more incidents are detailed.





administration expect this to include removal of agency perimeters? Is this part of the DHS roadmap for protecting agency traffic? How will DHS Einstein protections support agencies moving to public SaaS and cloud-based services? I just don't see how agencies will be able to deliver on this request.

#### CONCERN 4: SUPPLY CHAIN SECURITY

While I also applaud the correctness of targeting supply chain security, the order will politicize processes such as **Software Bill of Materials** (SBOM) which can be implemented by just including boilerplate in software contracts. It also includes technically unattainable goals such as attesting to the integrity and provenance of open source software. I'm just not sure how any group can possibly do that.

#### CONCERN 5: DETECTION, RESPONSE, AND REVIEW

While detection, response, and review are certainly important capabilities, the order basically demands that everyone do these things better. While one wonders why prevention was not also explicitly called out, the likely response to these demands will be a flood of new purchases of cyber security products. In fact, EDR is called out explicitly as a requirement, which is a massive gift to those vendors.

In the end – this Executive Order includes too much – and demands things our community has been demanding for decades with little success. I would have rather seen a one-sentence executive order demanding that every company in the Fortune 500 sponsor ten students for a free computer science BS degree in return for five years in the government. The result would be 5000 youngsters joining government each year, and that would have real impact.



*"...and this year's award for Best Malicious Actor in a Ransomware Attack goes to..."*



# WE NEED MORE SCIENCE IN CYBER SECURITY

DAVID HECHLER

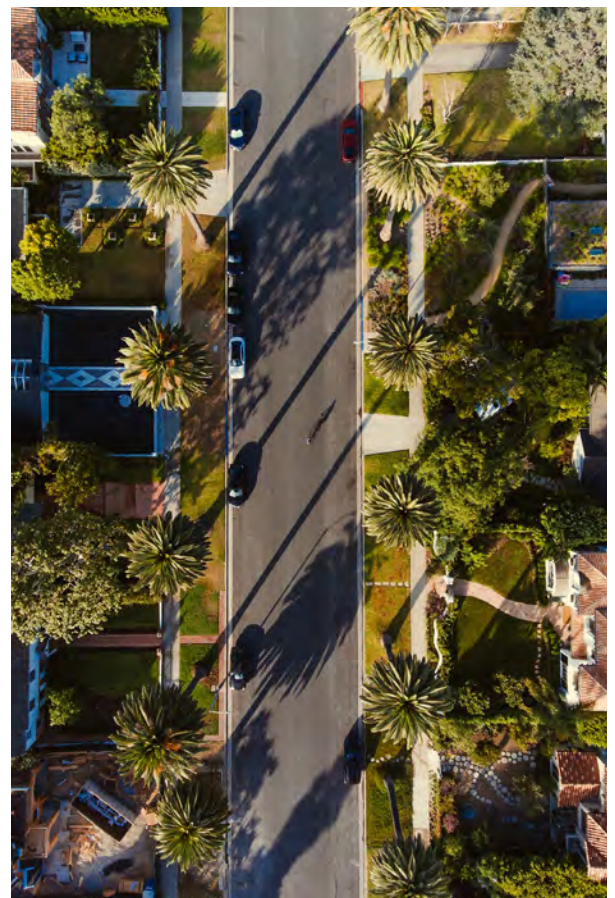
What struck me first about Terry Ingoldsby's approach to cyber security was the emphasis he placed on objectivity. Everyone knows that working in this area requires a combination of art and science, but Ingoldsby was tired of relying so heavily on the art side. He was a physics major in college, and he was looking for a sturdier foundation—even if it took years to find one (which it did).

As I dug deeper, I realized that his approach also raised important questions about the way companies think about cyber security. Is this a long-term challenge that requires time, attention, and resources from top executives? Or is it a continuing series of potholes that the company must maneuver around on the long information superhighway?

When we spoke on Zoom in late March, Ingoldsby first explained why he had hungered for objectivity. He had an analogy he used to explain what he meant. "No engineer worth their salt would ever build a bridge and wonder if it was going to hold," he said. But in essence, that's what professionals in IT security do. "We basically take our current budget and run out and buy stuff, plug it in, and turn it on. And pray that it will do something. And then, when it turns out that it wasn't enough, we get the next year's budget and we go out and buy more stuff."

This is not the way it should be, said Ingoldsby, who is founder and president of [Amenaza Technologies](#) in Calgary. (Amenaza is Spanish for "threat" or "menace.") When engineers are commissioned to build a bridge, they gather data. What will its dimensions be? What load must it bear? How many lanes will be required, and how much traffic will it draw? Then they build a model and check it, tweak it, test it. "And only when they're satisfied that the design is correct do they start ordering things and assembling them in accordance with the design," he said.

**"Most security stuff gets sold on fear. I mean, basically put terror in their hearts, and maybe they'll buy something,"**



This is what he wanted to incorporate into his work, and the big thing he was missing was data.

He has a clear recollection of when his quest began. In 1995 he started a consulting company to do system administration and network security for oil companies. He was often asked to undertake security assessments. The reports he produced were probably as good as those written by others in the field, but there was no more rigor to the work, he said, than searching for water with a divining rod. "I probably don't have enough training," he thought. So he signed up for conferences and made the rounds.

Two years later he heard security technologist **Bruce Schneier** give a talk about attack trees. "Suddenly the lights had come on," he said. The concept involved templates similar to decision trees. It was a way to calculate risk by assessing adversaries' capabilities and your own vulnerabilities. The end result is that attack trees helped you weigh the threat and determine countermeasures to fend off attacks.

Ingoldsby was excited. This seemed to be what he was looking for. After the talk, he approached Schneier and asked if there was software to implement his system. Unfortunately not, the security guru told him.

The next year, Schneier spoke at another conference and Ingoldsby buttonholed him again. Still no software? "No," Schneier told him. "That's why I'm giving these talks. I'm hoping that somebody will go out and write some." That was all Ingoldsby needed to hear. He told Schneier that he would be that somebody. He figured it would take a few weeks. "How hard can this be?"

Ingoldsby smiled before he continued. "Well, that was 20 years ago. And we're still improving and refining the software. So it kind of became my career." A career devoted to selling attack tree software.

## A DIFFERENT KIND OF PITCH

Even before he explained how it worked, I could see how different his pitch was from the usual way cyber security is marketed. It's almost the obverse. Nothing about the latest breaches "ripped from the headlines." Or the devastation of a ransomware attack. Usually there's a lot of subjectivity in the pitch. Fear is a powerful persuader.

I asked Ingoldsby about that. "Most security stuff gets sold on fear," he agreed. "I mean, basically put terror in their hearts, and maybe they'll buy something," he said. "From my perspective, if you're ever in the situation where you are now experiencing terror, it's already too late. At best, you're trying to pick up the pieces." The power of an objective approach is clearly an appeal to reason, which may be a harder sell, as Ingoldsby is well aware.

When it comes to sales, there are two big challenges he's run into. What he's selling is not designed to help the IT department fix the most immediate problems they face on any given day. Even when they purchase his software, it won't magically eliminate the to-do list of tasks they need to perform that week. It's a longer term investment. And the benefits of what he offers are likely to be most appealing to company executives and their general counsel rather than the IT department. But he has a hard time reaching them.

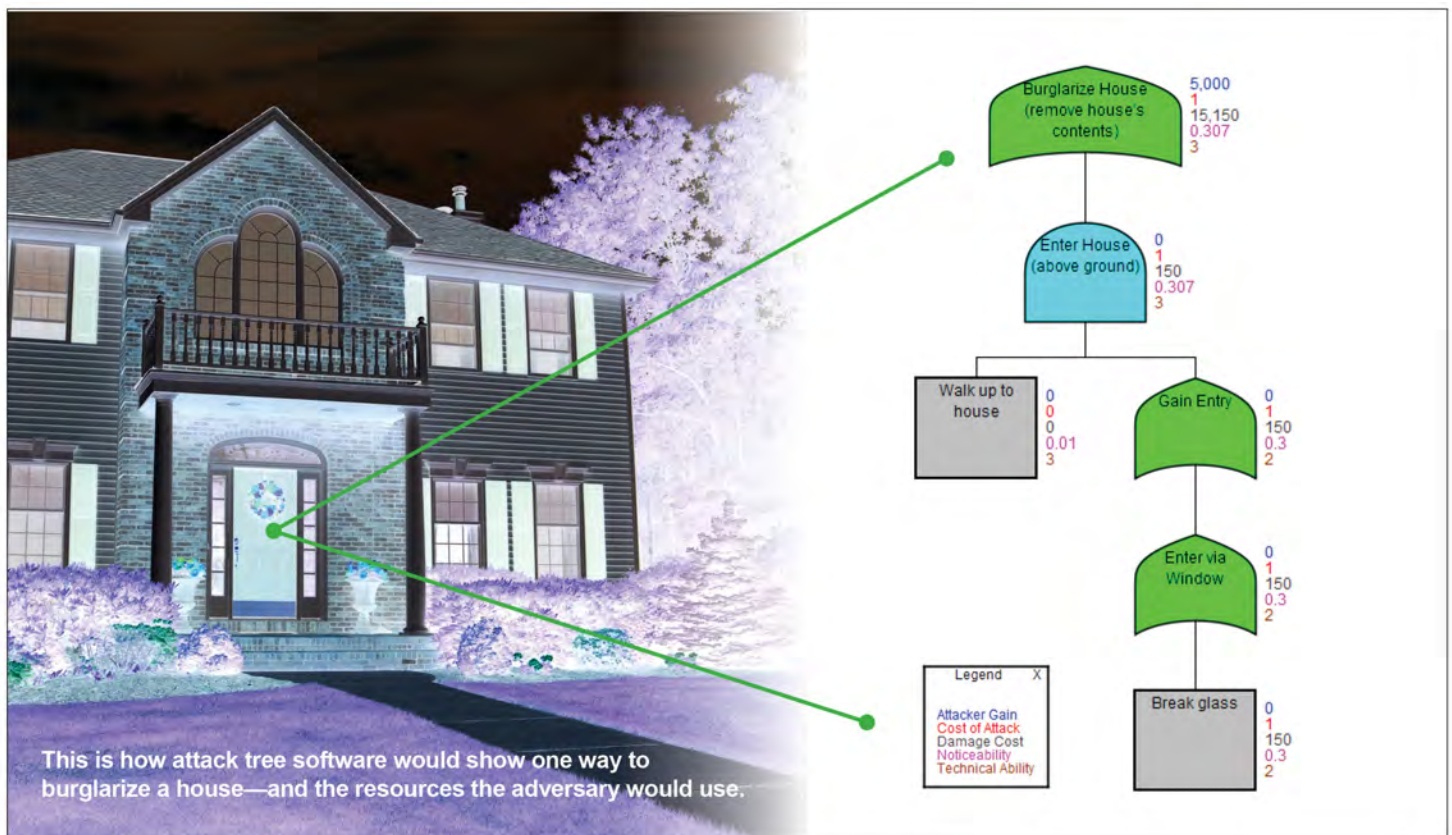
This is where I started to see that larger issue emerge. It's one of the biggest challenges in cyber security. So often a crisis comes down to the resources a company had devoted to this area and how

**"If you're ever in the situation where you are now experiencing terror, it's already too late. At best, you're trying to pick up the pieces."**

much attention its executives have been paying. They may say that cyber is not just an IT problem, but is that reflected in their behavior?

## HOW ATTACK TREES WORK

The Amenaza website has a page devoted to the [origin of attack trees](#). The most important piece was a 1998 [paper](#) co-authored by Schneier with research sponsored by the National Security Agency (where two of his co-authors worked). The full picture of their provenance is murky, Ingoldsby said, because they seemed to have been developed in classified environments. In the 1960s, “fault trees” were used to study unexplained missile failures. This seemed to be the earliest version of the concept. Next along the timeline, Edward Amoroso popped up (much to my surprise). The founder and CEO of TAG Cyber wrote about “threat trees” in a 1994 [book](#) he published when he was at Bell Labs. Ingoldsby wasn’t sure if Amoroso’s work was independent of the NSA’s, so I asked. Amoroso’s answer tied all the trees together. In the 1980s, his work on threat trees involved missiles, just as the earlier fault trees had. Amoroso’s work was related to the Star Wars missile defense program (aka the [Strategic Defense Initiative](#)). And the NSA was involved, he added.



After securing Schneier’s blessing at the second conference, Ingoldsby pulled together a small team to start building the software in late 1998. A few months later, Christine McLellan joined the effort and took charge of software development. The first version of the program, called SecuriTree (pronounced secure-i-tree), was born in 2000, and Amenaza Technologies was incorporated in January 2001. Two decades later, McLellan is still there as VP, product development.

Amenaza’s business is selling the software. Ingoldsby recommends that customers pay for a three-day training as well. It’s not just a matter of learning commands. Using the software is a learning experience—almost like taking a course. But it’s a different course for every company, because it



requires them to explore their own adversaries and their own vulnerabilities. And after the company's employees understand the concepts and how the program works, Ingoldsby usually spends the last day of the training helping them begin mapping their own security landscape.

When he explained the basics to me, Ingoldsby almost sounded like he was describing one of those brainy old board games, like [Avalon Hill's Gettysburg](#). Picture an upside down tree, he said. At the top is the root, which represents the goal the attacker seeks. Moving down we see processes and procedures that the attacker may adopt to get there. At the bottom are leaf exploits that offer possible ways to begin the voyage.

Attacks require resources. These include money to buy equipment, technical ability, physical access. Assessing them allows a company to calculate the overall cost. And this can be matched with the various types of adversaries to determine whether they're capable of an attack, how much they would benefit from it, and how likely they are to pursue a given path. A company can also calculate the cost to itself and build models that show which paths would be most devastating, and which less so.

Does this make your company secure? Ingoldsby asked and answered the question himself. "SecurITree is a tool in the same sense that Microsoft Excel is a tool," he said. "What does Excel do? If you double click on Excel, there it is in its glory. But it's not doing a thing for you. SecurITree allows you to make sense of what you know. It only reflects back what you tell it. But hopefully the way it reflects it back gives you enlightenment—reveals things to you that you didn't know that you understood."

## THE PAYOFF MAY NOT BE EXACTLY WHAT YOU EXPECT

Sometimes those revelations are not what customers expected. A lot of security work involves instinct and gut feelings, Ingoldsby said. And we have a tendency, he continued, to look for the kind of attack we might engineer if we were attacking ourselves. But that doesn't mean the attacker will agree. "So by having to construct this model, it kind of guides one's thinking to look at the bigger picture of how somebody else might take on your system."

One of Ingoldsby's favorite stories involved a client in the defense space. After their three-day training, the attack team returned to a problem they'd been working on for months. It involved military planes, which are apparently most vulnerable when they're sitting on the tarmac—or, in this case, on the decks of aircraft carriers. The group would meet for two hours and get nowhere.

This had been going on for four months. Then they constructed an attack tree to tackle the problem, and they realized what the impediment was. It was the terminology: "Oh, that's what you meant by that? That's not what I meant!" Using the software forced them to describe the attack scheme "in a mathematical fashion," Ingoldsby said, which eliminated the ambiguity. "They made more progress in two hours than they had in the previous four months."

There was one more benefit that Ingoldsby wanted to emphasize. And it's one that would naturally appeal to management and general counsel. In addition to the protections attack trees may help a company construct to protect its IT network, there's another kind of protection it can offer: a due diligence defense. "As you create these models," he noted, "you're essentially creating a document, in a mathematical fashion, of everything you considered and why you discounted certain things as not being a risk. Now, you might be wrong," he conceded, "but you will be able to explain that, 'Based on the knowledge we had at the time, it was a reasonable and rational decision.'"

And for executives and their lawyers, he added, that may be worth a lot.

# HAVE YOUR FRIENDS ASKED YOU ABOUT BLOCKCHAIN AND CRYPTOCURRENCY?

JENNIFER BAYUK

---

A friend of mine asked me for an opinion on what to read or which news channel to monitor to learn about blockchain and cryptocurrency, at the same time apologetically wondering, as I work in cyber security, if I knew anything about it. You probably get these as well. The most recent question sent to me was:

*"This may not be in your wheelhouse, but I thought I'd reach out to seek resources for wrapping my head around blockchain and cryptocurrency – books, lectures, whatever. If you have any ideas, I'd appreciate them."*

As a cyber security professional, both blockchain and cryptocurrency are firmly in my wheelhouse.

Blockchain is a technology that is used in multiple business applications, mostly financial, to keep track of business transactions and hold people accountable for changes to information. It creates a very hard to reproduce number for every change made to a multi-level transaction so it is possible to show with high probability that a given person or company authorized a change to data. It can be used to verify the integrity of any process wherein multiple parties participate in a step-by-step process and need incremental evidence to agree upon the outcome.

Because of this use case, it is the technology underlying cryptocurrency which, by contrast, is pretty much hype. Very much like gambling; the house always wins. One person or group creates the beginning of a blockchain, and there is no underlying value to it when you start, just a random hand of cards. One may argue that the dollar used to be based on a gold standard and it is no longer, but at least the dollar is still backed by the Federal Reserve. Neither the Federal Reserve nor any bank or financial institution guarantee to exchange cryptocurrency for real dollars. Those that purchase it are doing so on pure speculation.

Speculators are drawn to cryptocurrency because it is harder to track than regulated banking transactions

**Because there will always be a market for such nefarious activities, neophyte investors often think they can ride the tail of such investments, but for them it is simply rolling dice.**

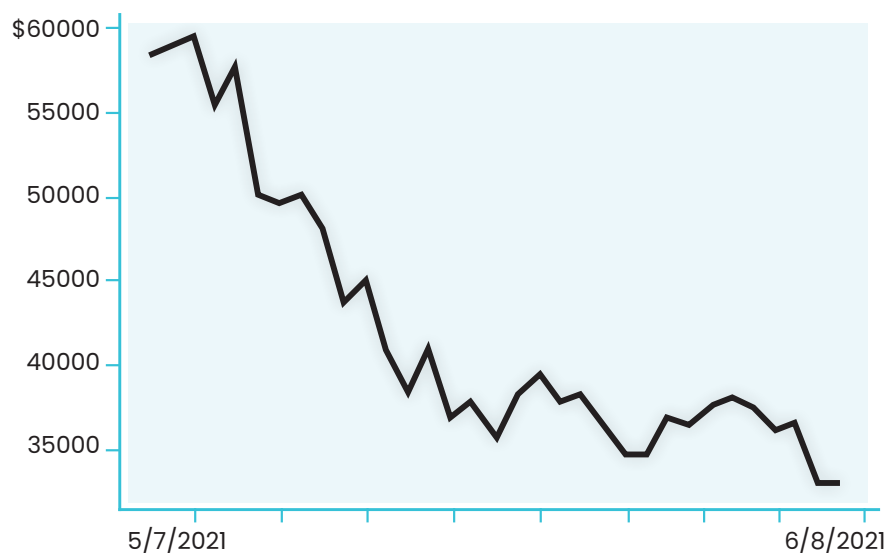


and therefore easier to evade monitoring of spending. There are non-nation-state organized (criminal money laundering) syndicates that swap real dollars for cryptocurrency so they can spend it as anonymously as possible with willing merchants who know that they can sell the cryptocurrency to other like-minded money launderers. Because there will always be a market for such nefarious activities, neophyte investors often think they can ride the tail of such investments, but for them it is simply rolling dice.

That said, the underlying technology of blockchain has helped government track money launderers, so transactions are not as secret as they used to be. The recent recovery of ransom paid by Colonial Pipeline to the DarkSide threat actor group is evidence of that.

Also, it has come to attention that cryptocurrency requires so much blockchain computing to operate that the data center electricity consumption is horribly bad for the environment. Recently Elon Musk announced that Tesla suspended vehicle purchases using Bitcoin out of concern for the environment. Unfortunately for Colonial Pipeline, their attack started on May 7, 2021 and Musk's announcement came on May 11. Market reaction to Musk's announcement was a dive in the value of Bitcoin that continued through May, so by the time the FBI recovered part of the Colonial Pipeline's Bitcoin ransom in June, it was only worth \$2.3M. For these types of reasons, there will be constant changes in the cryptocurrency ecosystem.

### Bitcoin Closing Prices in Colonial Pipeline Attack Timeframe



Source: [www.coindesk.com/price/bitcoin](http://www.coindesk.com/price/bitcoin)

Bottom line, a legitimate technology company selling blockchain-based software to the healthcare or insurance industry may be a good investment, but a cryptocurrency is emphatically not. That said, nation-states and national banks are dipping their toes in the water, and if our national currency makes the leap, we will all have to follow.

All that said, my friend simply asked what would make sense to read. The Economist had a good set of articles on blockchain and cryptocurrency the first few weeks of May, but whatever you read, read it through this lens.



An aerial photograph of a small, rocky island surrounded by dark water. The island is densely covered with trees, many of which have turned vibrant shades of yellow, orange, and red, indicating autumn. Some trees are still green. The rocks are grey and jagged, protruding from the island's surface. The overall scene is captured from a high angle, looking down on the island.

# INTERVIEWS





## AN INTERVIEW WITH DAVID RATNER, CEO, HYAS

# PROTECT YOUR NETWORK WITH DNS DATA

SOC analysts are overburdened with data. This “noise” makes it difficult for them to decipher which indicators of compromise (IoCs) are actionable and which are priority. Without the data, however, understanding what bad actors are doing, where they are, which domains and infrastructure they’re using, etc., is impossible.

While SOC tools may spin out terabytes of data per day, DNS data remains one of the lesser used categories of data for threat intelligence, investigations, incident response, or contextualization. However, DNS data is a rich source of information that allows companies to identify bad actors and the domains they are using to execute attacks. It allows defenders to monitor adversary campaigns and prevent attacks. As such, PDNS — protective DNS — is becoming a key capability that even the U.S. government is getting behind.

HYAS, a PDNS provider based in Victoria, Canada is helping companies identify adversary infrastructure and communications. We spoke with David Ratner, CEO at HYAS, about this growing space.


**TAG Cyber:** *The NSA and CISA just issued guidance about incorporating DNS data into security operations. Why did this happen now?*

**HYAS:** 2020 was an interesting year for a variety of reasons, but one thing that happened was the rapidly changing work models created a dramatically expanded attack surface. This, combined with a set of high-profile supply chain and ransomware attacks, made people realize that, despite all the investment in cyber security, organizations were not as protected as they needed to be. Organizations needed to be more proactive and focus on prevention vs. incident response — they need to move away from traditional defense to active defense. Looking at the DNS egress of an organization is a key part of interrupting the kill chain and stopping attacks before they start. Detecting communication with command-and-control (C2) structures and acting on changes to an organization’s “DNS fingerprint” are the early warning signals that should be immediately integrated into a modern security architecture for advanced security.

**TAG Cyber:** *Why don’t companies use DNS more readily as a data source for identifying IoCs?*

**HYAS:** DNS is often a part of the infrastructure that “just works” and people may be either unwilling to touch it, lest they accidentally break something critical, or may not fully understand it, and therefore be unsure about how to properly effect change. Nevertheless, it’s vital to understand the role it plays in modern attacks, from ransomware to malware, supply chain attacks, and even phishing. Most attacks, regardless of how the bad actor establishes their initial foothold inside the network, utilize communication between some program or malware inside the organization and the bad actor’s C2 infrastructure outside the enterprise.

**It's exactly this kind of communication which shows up loud and clear when looking at DNS egress and specifically at "what changed, why did it change, and what does this mean."**



For instance, in a ransomware attack, Cobalt Strike or other sophisticated software is often deployed to navigate the enterprise and identify the best location in which to deploy the ransomware. It's exactly this kind of communication which shows up loud and clear when looking at DNS egress and specifically at "what changed, why did it change, and what does this mean."

***TAG Cyber: What are the top use cases for incorporating PDNS into an enterprise security program?***

**HYAS:** A key use case for protective DNS is visibility — one of my mentors used to tell me that you can't expect the right thing to happen for anything that you don't inspect, and if you aren't inspecting where your outbound traffic is going, you lack the visibility to understand what's happening on your network. Visibility could include knowledge about active infections, suspicious or unwanted network traffic, or even other network events that are leading indicators of something nefarious — for example, if the number of lookups for "no-such-domain" skyrockets one day, or the number of direct-to-IP communication is suddenly a lot larger, that points at something new in the organization that needs to be investigated, at least.

A second key use case is compliance. For example, NIST recently released NIST SP 1800-30B "Securing Telehealth Remote Patient Monitoring Ecosystem," where they recommend the use of a protective DNS solution. Additionally, having the proper protective DNS solution in place is also a requirement for CMMC Compliance, specifically under standard SC.3.192.

***TAG Cyber: Tell us a little about HYAS Insight and HYAS Protect.***

**HYAS:** HYAS, the expert in adversary infrastructure and the communication with it, focuses on using our knowledge to not only disrupt and detect attacks, but help our customers change the game, avoid playing traditional defense, and stop attacks before they happen by being proactive.

HYAS Insight is used by Fortune 100 organizations around the world not just to rapidly understand "what happened," but also identify everything needed to counter fraud or understand an attack and either involve law enforcement or adapt one's defenses to proactively get in front of future attacks by the organization — the first step in an active defense is knowing one's enemy.

HYAS Protect is an automatic protective DNS solution that uses all the same data to proactively extend a "protective shield" around an organization by analyzing the DNS traffic in real time and being able to block and/or alert on untrusted or nefarious communication. It can run as an organization's external DNS resolver, be integrated with third-party agents on devices to address hybrid work-models, and is flexible enough to be easily



integrated into a security architecture without having to act as the external DNS resolver.

Both HYAS Insight and HYAS Protect are SaaS solutions that can be API-integrated into commercial and proprietary solutions and are deployable in minutes with minimal if any configuration and maintenance required.

***TAG Cyber: What some of the things that DNS data can tell analysts that other security data cannot?***

**HYAS:** First and foremost, DNS data can tell analysts what conversations are happening between their organization and the outside world – understanding where devices in the network are communicating is a critical first step to understanding what may need additional inspection and analysis. While protective DNS is not a zero trust solution, evaluating the validity and trustworthiness of any network connection is clearly an important part of an overall zero trust approach.

Second, DNS data can also tell analysts what network traffic is being attempted, which even if not successful can often identify suspicious or nefarious internal activity – great examples are sudden increases in lookups on invalid domain names or direct-to-IP traffic (which will often appear as a DNS lookup on an in-addr.arpa address).

In general, analyzing the DNS data provides an analyst with high-fidelity leading indicators before bad things happen, and often provide advanced data points on where to more deeply inspect inside the organization. One of the more difficult things an analyst has to do is prioritize their work in an environment with competing priorities. Protective DNS provides high-confidence data that won't waste their time. The use of DNS data from a protective DNS solution like HYAS Protect provides a strong signal with a low false-positive rate that allows analysts to optimize their time and focus on the real issues for next-generation protection.



AN INTERVIEW WITH MICHAEL CICHON,  
CHIEF MARKETING OFFICER, IKOSMOS

# CONVENIENCE, PRIVACY, AND SECURITY WITH PASSWORDLESS AUTHENTICATION

Digital identity and assurance are challenges in the modern world. Where a user might have one identity for work, they might have additional, similar-but-not-exact replica identities for personal use. Even those identities can vary: A person's true identity might be necessary when applying for a bank loan but not necessary when they are using social media or shopping online.

Businesses thus have to authenticate claimed identities and ensure that the user is valid and authorized. In recent years, businesses have begun to move away from the outdated username + password combination for identification because it is not a good method of assuring digital proof. Instead, passwordless authentication and identity proofing has taken hold in B2C and B2B companies alike.

IKosmos, a digital identity platform provider, is helping lead the charge with their BlockID solution. Michael Cichon, Chief Marketing Officer at IKosmos, spoke with TAG Cyber about how passwordless, behavior-based solutions are helping to prevent fraud and cyber compromise.

***TAG Cyber: What is BlockID and why is it necessary?***

**IKOSMOS:** BlockID is a FIDO2 and NIST 800-63-3 certified distributed digital identity platform supporting both business-to-employee and business-to-consumer services such as employee and contractor onboarding, Know Your Customer (KYC) identity verification, and multi-factor authentication. It provides individuals with a secure digital identity they control and that service providers use with consent to fight identity fraud.

Users like it because it offers the convenience of biometric authentication and eliminates the need for passwords, one-time codes, and other methods of authentication that disrupt their workflow. Security and IAM professionals like it because it easily integrates with existing operating systems, applications, and IT security infrastructure such as SSO via standard API/SDK.

***TAG Cyber: What are some of the cleverer ways you've seen threat actors commit fraud in recent months?***

**IKOSMOS:** Most recently the ransomware attacks at JBS and Colonial Pipeline, and SolarWinds before them, have reminded us of the vulnerabilities passwords represent. The recent Executive Order on Improving the Nation's Cybersecurity stressed the importance of using multi-factor authentication to shore up passwords. The unfortunate reality is that passwords were never intended for modern day internet workloads. Most working age adults have dozens to hundreds of passwords that need to be remembered in combination with a user ID and service, but at the same time are unguessable and need to be changed regularly.

**We used the best technologies available to accommodate privacy and security in addition to achieving interoperability and end user convenience.**



Employees' and consumers' needs for workarounds is obvious. As a result, people cache them in browsers, save them in keychains, and hide them behind SSO. But as a shared secret with the service providers, they need to be protected. However, despite billions invested in security, password-based attacks continue to be successful.

The debate now seems less about the need to replace them than how to go about it; nearly every system and every individual employee and consumer is affected. Clearly, this will not happen overnight or evenly across the enterprise.

While vendors quickly rush to market with passwordless authentication solutions, IT practitioners need to evaluate which ones will provide durable benefits – for to users in the form of convenience and privacy, and to organizations in the form of efficacy, security, and cost.

***TAG Cyber: Which identity-related regulations and standards are emerging that businesses must be aware of?***

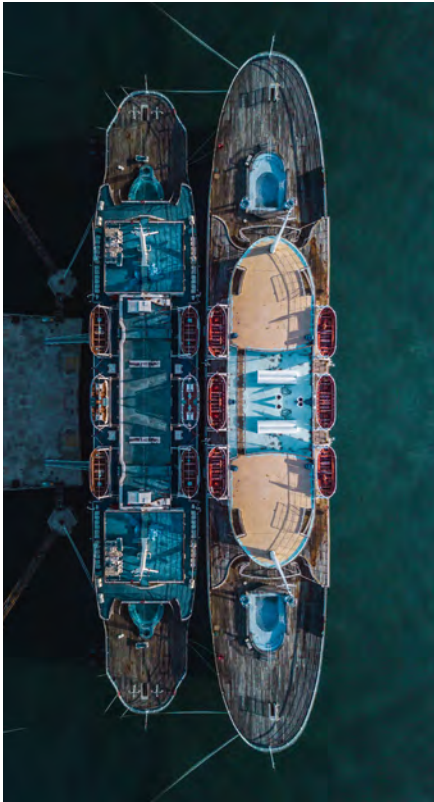
**IKOSMOS:** In the U.S., the 2001 Patriot Act and similar regulations passed globally have led to the formulation of KYC guidelines that banks and financial institutions must follow. This, in turn, has spawned follow-on security guidelines such as NIST 800-63-3, which defines specifications for asserting and authenticating identity, particularly in a remote setting.

It's clear that solutions performing biometric identity proofing and authentication need certification to this NIST standard in order to fulfill KYC compliance.

In Europe, we've seen the PSD2 regulations finally take effect and a move toward open banking in the UK. These largely require payment transactions to be dynamically authenticated with strong customer authentication in the form of multi-factor authentication. Here the European Banking Authority (EBA) has been very specific about what counts as suitable "inheritance elements" (what you are), "possession elements" (what you have), and "knowledge elements" (what you know) to claim compliance.

Finally, the Fast Identity Online Alliance (FIDO) has defined their FIDO2 standard laying out requirements for strong authentication of user logins and cryptographically signed transactions using biometrics and private-public key pairs. This, combined with existing GDPR privacy regulations, needs to be considered when businesses evaluate their requirements for going passwordless.





***TAG Cyber: Your system captures numerous attributes of identity, including biometrics (face, voice), PII, and government-issued documents. Doesn't adding more identity attributes actually increase risk of compromise against a consumer?***

**IKOSMOS:** We took a clean slate approach to developing our platform. We used the best technologies available to accommodate privacy and security in addition to achieving interoperability and end user convenience. Our platform was then developed to comply with the strictest GDPR, SOC2, and ISO 27001 standards for handling and retention of sensitive data.

Specific to the identity attributes, these are stored in a distributed ledger to W3C DID specifications and accessible only via a FIDO2 certified private-public cryptographic key pairs in which the private key is stored on the user's device (Secure Enclave) and cannot be accessed by anyone else, while the corresponding public key is stored on IKosmos Cloud infrastructure.

Instead of taking a password to gain access, the individual uses their own biometric and device. This eliminates centralized information storage and honeypots of stored shared secrets. There is no password to attack and no central authority managing access.

***TAG Cyber: What are the top use cases for BlockID?***

**IKOSMOS:** There are several that surface on both the workforce and customer sides of the business.

1. We address identity proofing requirements for employee verification (e.g., I-9) during hiring. This alleviates significant administrative workload, accelerates onboarding and improves security.
2. Authenticating remote workers for access to online services through the use of multi-factor authentication also rises to the top.

Other worker-facing use cases include adding identity proofing and biometric authentication to single sign-on, managing physical access to corporate facilities, and supporting zero trust strategies with minimal friction, including app-less authentication for organizations that prefer a zero-code footprint on end user devices.

A few of the more significant use cases on the customer side include identity proofing for KYC compliance, passwordless biometric authentication for logins, and strong customer authentication in support of PSD2. We implement via standard APIs and are a certified full services NIST 800-63-3 provider in support of portable customer identity and open banking requirements.



AN INTERVIEW WITH JOSH LOSPINOSO,  
CEO, SHIFT5

# SECURING CRITICAL INFRASTRUCTURE VIA OBSERVABILITY

The recent attack on Colonial Pipeline is another stark reminder that critical infrastructure (CI) is a prime target for threat actors. CI attacks are attractive to criminal groups because they make social and political statements and because CI components remain largely insecure. The migration from analog to digital systems and components in CI isn't new. Still, the problems of securing them linger since they don't operate in the same way as IT components. Plus, the requirements for their use are vastly different.

Digital CI components communicate over data buses and they generate tremendous amounts of data. However, communications over data buses are insecure, presenting a vulnerability primed for malicious exploit. Shift5, a security company led by former military cyber security experts, is helping CI companies run smarter, safer, and more efficiently, and giving customers a way to operate threat hunting programs that mitigate the threat of cyber attack.

Josh Lospinoso, CEO at Shift5, sat down with us for a conversation around this important topic.

***TAG Cyber: Tell us a little about the background and founding of Shift5.***

**SHIFT5:** The Shift5 founding team spent a combined 30 years in the US Army, where we were part of the founding group of Army Cyber Officers. We pioneered cyber security risk assessments on military weapon systems, which culminated in an important US Government Accountability Office report in 2018.


When information technology systems came to prominence in the 1970s, they were designed for reliability but not for security (e.g., ethernet). For 50 years, we've been dealing with the ramifications of that design choice by bolting cyber security onto the side of these IT systems. CI systems like fleet assets have also benefited from a digital revolution, albeit much quieter than in IT systems. (The first microprocessor was actually invented for the F-14 Tomcat fighter jet.) Unfortunately, we haven't seen a parallel narrative in the cyber security evolution of CI systems to that of IT systems.

The founding team left military service to step into this vacuum. Our thesis is that the inherent cyber vulnerabilities in CI systems is part of a broader category of problem: observability. By collecting data off these systems and nurturing an ecosystem of data scientists and software engineers who can harness that data, we can significantly reduce cyber risk, improve operational efficiency, and revolutionize maintenance. We set out to build this ecosystem.

***TAG Cyber: What are some of the technical problems of securing CI systems?***

**SHIFT5:** In general, CI systems are tough to secure because they are safety critical. When we design

## We believe that expensive fleet assets will be the next frontier of cyber attacks from cyber criminals.



security control measures to improve the cyber security of these systems, there's generally no appetite for increasing risks to safety or availability. So the appetite for false positives that create outages or safety hazards is zero.

Additionally, these systems are distinct from IT systems. So cyber security professionals working on these systems must draw lessons and analogies from IT cyber security while balancing a whole new set of protocols, systems, operational constraints, and attack vectors. This also makes it hard for cyber security companies to recruit and retain talent that has experience with or exposure to CI systems. Most cyber security professionals know Windows/Linux/Mac and IP over ethernet very well — not so much when we're talking about real time operating systems and serial data buses.

Finally, each CI system is bespoke. While an endpoint security product or a network intrusion detection system on an IT network can rely on a stable Windows API or broad compliance with networking RFCs, there's much less of this similarity across CI systems like fleet assets. This creates a scale challenge for cyber companies wanting to have broad applicability.

### ***TAG Cyber: How is Shift5's approach different from that of other CI security companies?***

**SHIFT5:** The most apparent difference is that we're not just a security company. We're building an observability platform which supports a wide range of use cases that includes cyber security. This larger vision allows us to appeal to fleet operators both security conscious and otherwise. If we're able to defend your fleet assets against a latent and largely unrecognized cyber vulnerability, that's great. But it's even better when we can save significant fuel costs or substantially increase fleet readiness.

We're also different in that we're segment agnostic. We focus on fleet assets — planes, trains, and tanks — and these span many markets like rail, maritime, aerospace, and military. This depth permits us to draw from the lessons we learn from one segment and apply those to the others.

### ***TAG Cyber: Shift5 has a refined focus on a subset of CI organizations. Why did you choose those industries?***

**SHIFT5:** There are trillions of dollars of fleet assets in service around the world. For a variety of reasons, they've received relatively little attention from the cyber security community. Our founding team has combined decades of experience working with these important, multi-million-dollar assets, and we believe that they are catastrophically underserved; the market is big enough for a robust platform to be built.





We've focused on these high-end fleet assets because (a) there's enough similarity across the platforms to permit significant scale, (b) the unit economics for the asset owners are very attractive, and (c) we believe that expensive fleet assets will be the next frontier of cyber attacks from cyber criminals. Many smart, well-funded entrepreneurs are tackling the IoT and ICS/SCADA spaces and it's crucial that they're successful. For us, we believe that fleet assets are a large and complementary class of CI that is in dire need of what we're building.

***TAG Cyber: We all know what happen with Colonial Pipeline. Given your insights into the space, what's next? What types or targets of attack are highly probable?***

**SHIFT5:** What we're seeing right now is that relatively unsophisticated ransomware attacks on IT are having cyber-physical effects. The bar is really low for criminals to have profound effects on CI because the security posture isn't sufficient.

As the cyber security community improves these CI systems, we'll invariably see a shift towards other low-hanging fruit. Unfortunately, criminals have now learned that holding CI hostage can be very lucrative. The Colonial attack alone resulted in a \$4.4M ransomware payment.

A few weeks ago the New York MTA was also hacked. We're assured that rider safety wasn't put at risk and that the train cars themselves were unaffected, but in general these fleet systems are imminently vulnerable. What happens when a cyber criminal disables a fleet until an operator pays a ransom? Or worse, threatens to put people or cargo at risk?

We aren't the only ones thinking about these inevitabilities, but we're at the frontier of securing these systems for when criminals invariably move on to these critical systems.



AN INTERVIEW WITH TOMMY TODD,  
VICE PRESIDENT OF SECURITY, CODE42

## CAN YOU QUANTIFY YOUR INSIDER DATA RISK?

It's safe to say that the ways in which people work have changed more rapidly in the preceding 15+ months than in another condensed time period in history. These changes have necessitated a fresh look at data: where it resides, how users access it, and the controls by which security teams protect it. Yet, it's not just the data, itself, that poses a risk — although data remains the target of cyber adversaries.

Rather, given workplace changes and the need for users to move faster and more efficiently, security teams are rethinking the risks of human access to and use of data, a.k.a., "insider risk" or "insider data risk."

Code42, a provider of insider risk detection and mitigation, is helping enterprises look holistically at their insider risk and data protection strategies and processes. Tommy Todd, Vice President of Security at Code42, spoke with us about data risk protection and how this category is different from your grandparents' DLP, behavioral monitoring, and even endpoint detection and response.

***TAG Cyber: How have data access and use changed in the last year?***

**CODE42:** As a result of the working from home conditions that have impacted the entire world, we have seen data become more distributed. This, in turn, changes the way employees access, share, and consume information. The increased reliance on collaboration tools, more data being created outside the "traditional" network perimeter than before the pandemic, and the speed at which business is being conducted all contribute to a greater risk of data being exposed to potential unauthorized access and exploit. The possible consequences of a data breach could be significant — in terms of cost, reputation, and the ability to operate.

***TAG Cyber: Is there really more risk to companies as it pertains to data or is this a perceived loss of control because employees are not working in offices and they're using (sometimes) unmanaged devices and unsanctioned apps?***

**CODE42:** According to a recent commissioned study by Code42, insider risk management (IRM) is of greater concern now for 74% of companies than it was before the pandemic. Some of the key finding in this survey of 202 security professionals in the US who are "highly involved" with data loss prevent and incident response include:

- 66% of respondents experience data leaks due to insiders at least monthly.
- 82% of security professionals identify protecting sensitive company and customer data as a top priority.
- 71% of respondents agree that traditional approaches to DLP aren't working.

**Given that studies have shown up to 70% of all employees have admitted to taking data from one organization to another, departing employees are the greatest risk to data exfiltration for an organization.**



Clearly, the concerns are well warranted. This isn't perceived risk; it's real. And even as employees return to the office, the reality is that we are going to be faced with increasingly hybrid work environments (resulting in new, possibly ephemeral access requirements) and work turnover (meaning, the potential for more disgruntled employees on their way out of the organization and the introduction of new, as-yet-untrusted insiders with access to data). Both scenarios will no doubt increase the risks associated with insiders.

***TAG Cyber: DLP has been around for a long time and many companies use it but still deem it ineffective. How does Code42 approach data risk differently?***

**CODE42:** Data risk assessments should start with visibility into all data vs. just looking at a subset of classified data. By focusing on all data and offering a view of risk across files, vectors, and users, Code42 provides the necessary holistic view required to approach data risk. For companies still using DLP, many of them simply have it on in maintenance mode because of the sheer number of false-positive alerts triggered in a given day. Code42's context-rich alerts are fewer in numbers but provide the necessary context for organizations to frame the appropriate right-size response. How organizations respond to context is key because again, in a DLP world, the outright response of blocking is no longer acceptable to today's cloud-based and remote workforce. Productivity coupled with data protection is key.

***TAG Cyber: When or where is data most at risk?***

**CODE42:** Data exposure risk is increased through a number of factors, not all of them being malicious in nature. However, given that studies have shown up to 70% of all employees have admitted to taking data from one organization to another, departing employees are the greatest risk to data exfiltration for an organization. This is of particular concern now as the economy works its way out of the pandemic. We can expect job hopping to a degree never seen before, remote work scenarios causing all sorts of security headaches and turnover. All of this creates a situation of uncertainty which, in turn, leads to risk.

***TAG Cyber: What are the key signals of an insider data threat?***

**CODE42:** Insider risk indicators often include areas such as unusual spikes in data movement, premeditated employee departure activity, file type mismatch activity where the file extension is changed in an effort to circumvent policy, and mirror IT usage where the user is just one click away from potentially putting data at risk. The key here is to focus on the story being told by the data and user. If there are changes made to a file, along with where that file is being moved and when the user might be doing all of this, these could potentially indicate an insider data threat. Following the data (as opposed to the user) is generally the best place to start picking up those signals.





## AN INTERVIEW WITH TONY PEPPER, CEO, EGRESS SOFTWARE

# ELEVATED EMAIL THREATS? NOT WITH HUMAN LAYER SECURITY

Email is the primary way in which businesses communicate, especially in the age of remote and hybrid work. When it comes to companies' supply chains — partners and suppliers — a good deal of sensitive information is exchanged via this digital channel.

Anyone working in cyber security knows that email is a highly susceptible threat vector. Attackers prey on human error and busyness to affect breaches, and when it comes to the supply chain, they know information like financial data is up for grabs if executed correctly. Unfortunately, email-based compromises persist because many traditional email security tools cannot accurately detect attack attempts, and an even fewer focus on human behavior, the so-called "human layer," as part of detection and prevention.

Egress Software, a provider of intelligence email security solutions, is using the human element and advanced detection to help stop email threats, even when the compromise starts in the supply chain. Tony Pepper, CEO at Egress, spoke to TAG Cyber about stopping email-based attacks.

***TAG Cyber: Phishing and business email compromise are nothing new; why is the supply chain becoming such a big consideration in email exploit?***

**EGRESS:** Inbound email threats including phishing, spear phishing, and business email compromise are certainly nothing new, but market conditions over the last 18 months have undoubtedly elevated the risk, and this is not just limited to supply chain.

The rapid transition to remote or hybrid working combined with huge investment in digital transformation projects because of the global pandemic have exacerbated vulnerabilities that always existed. A distracted and stressed workforce makes people more susceptible to a targeted attack. This elevated human risk factor combined with more sensitive digital data means the gains for cyber criminals have never been so great.

As the SolarWinds attack showed, the supply chain is a high-profile and potentially less protected target. Attackers are constantly developing new attack strategies and have more resources and tools at their disposal than ever before! For businesses, these attacks can be extremely hard to spot; it's easier to deceive people when you're pretending to be a trusted source. This is typically done using compromised email addresses and leveraging established relationships. But as demonstrated by SolarWinds, there are many ways to launch an attack from within the supply chain.

The headline-grabbing attacks have certainly increased awareness of the risks, but volume of incidents continues to go up as organizations struggle to mitigate threats. Businesses need to

In a recent survey we conducted,\* more than 90% of respondents said they are more concerned by the legal actions following a breach than any regulatory misdemeanor or fine.



adopt zero trust models that assume by default all communication represents risk, whether using trusted credentials or not!

***TAG Cyber: What are the compliance issues or industry standards driving a focus on email-based cyber attacks?***

**EGRESS:** Regulation and industry standards have always been a factor. Now, at a time of heightened cyber risk, we also see something of tipping point in regulatory laws. In North America, CCPA has driven action in breach response, whilst other states consider their positions on data protection. At a federal level, the debate continues as to whether the US needs a set of national regulations.

At the same time in Europe, the fallout of the UK leaving the EU continues to be felt as countries try to comprehend the impact on data sharing. An adequacy status is likely to be agreed, but for many organizations both in North America and Europe, the operational impacts are yet to be fully understood.

The result is a confused regulatory picture. Yet, these are not the only factors pushing organizations to prioritize cyber risk reduction. In a recent **survey** we conducted,\* more than 90% of respondents said they are more concerned by the legal actions following a breach than any regulatory misdemeanor or fine.

***TAG Cyber: We know that at the beginning of the pandemic (i.e., work-from-home), email volume increased by nearly 95%, ratcheting up risk exponentially. Does that risk remain? Are there other threats you're seeing related to email compromise now that we're in a steadier state?***

**EGRESS:** The risk remains. In fact, as the workplace conversation pivots to allow companies to embrace hybrid working, the risk is increasing. Organizations are developing strategies to allow their employees time in the office whilst also retaining the lifestyle and flexibility benefits gained through remote working. As a result, workforces are more disrupted than ever. Working across numerous locations, accessing corporate email, data, and networks on multiple devices heightens the likelihood of human-activated breaches. These could be incidents caused by simple mistakes, for example, sending an email containing sensitive data to the wrong recipient or clicking on a link in a phishing email. Regardless of the cause, the breach can be equally damaging.

It is therefore no surprise that rates of phishing and subsequent ransomware attacks are rising quickly. Cyber criminals are aware of how vulnerable organizations and their employees are and are capitalizing on this. Equally, businesses and regulators acknowledge that human error accounts for as many data breaches as inbound attacks.

***TAG Cyber: How does Egress discover email risk?***

**EGRESS:** Against the backdrop of heightened risk and data breaches, Egress provides human layer security that uses intelligent technology to mitigate both inbound and outbound email security risks.

We understand that people get hacked, make mistakes, and break the rules. This understanding of human fallibility allows us to develop cyber security solutions that use contextual machine learning and natural language processing technologies to detect and prevent abnormal human behavior, such as targeted phishing attacks, misdirected emails, and data exfiltration.

From a discovery and detection perspective, Egress Defend identifies inbound threats based on a combination of factors. We take a zero trust approach that assumes every email is untrustworthy. We then analyze linguistic and contextual factors, reverse engineer how phishing emails have been created, and apply one-to-many detection to every email entering the organization.

From an outbound email risk perspective, Egress Prevent provides fine-grained reporting to identify human-activated incidents, including misdirected emails, insecure domains, and large recipient lists.

***TAG Cyber: What can businesses do, aside from implementing intelligent email security, to decrease risk (i.e., from a process or training perspective)?***

**EGRESS:** If organizations really hope to minimize email-based security risk, they first must acknowledge that the problem starts with their people. Their employees, their supply chain, and their customers. The risk is a very human one, and to protect against it, security solutions cannot be viewed in isolation. Technology and greater employee and supply chain awareness and education must go hand-in-hand.

Many information security professionals may perceive people in their business as their greatest vulnerability because they are so susceptible to causing human-activated breaches. But because of the complexity of the challenge to mitigate insider risk, they've not previously been able to patch this vulnerability.

At Egress, we believe that when armed with intelligent security tools, and a good understanding of the risks and ways to mitigate them, employees can become an organization's greatest defense. Get this combination right and the cultural change can be transformational. Suddenly, the compliance and security teams do not sit in silo; they become central to the wider organizational success. And in turn, employees feel empowered to get on with their jobs, whilst having the confidence that they can work securely.





AN INTERVIEW WITH LEON WARD, VICE PRESIDENT,  
PRODUCT MANAGEMENT, THREATQUOTIENT

## LEARN FROM YOUR DATA TO IMPROVE DETECTION AND RESPONSE

Security operations is all about efficiency. With the barrage of tools, alerts, and threats operators must manage on a daily basis, it is imperative to reduce as much manual work as is possible through automation of low-level tasks. Data collection, aggregation, correlation, contextualization, and enrichment are all tasks that call out for efficiency. Furthermore, operators crave the ability to pull together all this threat data from disparate systems and create one, unified view into enterprise threats, then have the option of initiating a response from the same platform. The key? Having the right data.

Efficient and effective threat detection and response (TDR) is table stakes. But finding the right tools proves challenging for some enterprises. ThreatQuotient, long known for its threat intelligence solutions, has followed the evolution of SecOps needs over the years and has enhanced its offering to include SOAR and XDR capabilities. Recently, we spoke with Leon Ward, Vice President, Product Management at ThreatQuotient, about the company's latest offering, ThreatQ TDR Orchestrator.

**TAG Cyber:** *A key element of TDR Orchestrator is automation. A lot of people think automation is simply offloading repetitive tasks. ThreatQuotient says that's a misconception. Why?*


**THREATQUOTIENT:** Actually I don't really think that it's a misconception as such, since that actually reflects how people use automation today; my position is that we need to evolve from this limitation and extract more value from automation in a security operations environment.

Existing approaches to security automation are great for repetitive tasks, but to actually apply automation to detection and response needs, one needs to focus on data and not the processes — we think that's radically different in terms of approach. So what if you've doubled your capacity to lookup more hashes in VirusTotal per hour or can execute more things in a sandbox faster? What does that get you? The important thing is not the fact that the action is performed, instead, the important thing is what a system has learned by performing those actions. We're building an approach that instead focuses on that data learned, and believe that it should result in much more detection and response value.

**TAG Cyber:** *ThreatQuotient has always been all about the data. Is there ever an argument that too much data complicates threat management?*

**THREATQUOTIENT:** Oh yes, you bet there has been! I've lost count of the number of times in my career someone has told me about their crazy massive store of security data... but having data is only useful if you can put it to use. Junk data consumes resources, slows down your ability

While automation can be seen as optimizing user time or resources, it alone can't ever impact the social aspects of keeping a workforce healthy and functioning well.



to find the needles in a haystack, and can become a lifecycle management headache that is best avoided. Prioritize what is important, store what you need, and keep within the limits of what is really possible in terms of people, process, and technology. One of our goals is to decrease the data that users need to care about, and therefore improve their focus.

***TAG Cyber: What are the biggest challenges SecOps teams are struggling with today, especially as the world is starting to shift from home-based work to hybrid work?***

**THREATQUOTIENT:** In addition to the classic SecOps special challenges, like too much work, super-complex problems, fighting an arms race of exploitation, vulnerability, and evolving techniques, don't forget that at their heart, SecOps teams are people. Those people are facing all of the same challenges that non-security teams experience, and it's easy for these challenges to be ignored by parts of the SecOps community.

It's really hard adjusting to remote working environments when you're not used to it. That hour or so of vital headspace downtime that a daily commute brings to many is suddenly removed, the time spent physically moving between meeting rooms or buildings disappears. While this immediately looks like optimization for being able to squeeze more zoom meetings into a day, or opening more time to focus on closing out tickets, researching incidents, or what have you, it can take its toll. A sprint needs to end, otherwise, it's a badly managed marathon.

So, while automation can be seen as optimizing user time or resources, it alone can't ever impact the social aspects of keeping a workforce healthy and functioning well.

***TAG Cyber: What threat actor trends are you seeing emerge?***

**THREATQUOTIENT:** I don't think there are any new trends that haven't already been identified and talked about extensively by others. Actors continue to use the same approaches that have been seen to work well, the supply chain looks an attractive target, and there is no shortage of new vulnerabilities with high impact out there to exploit in order to achieve their goals. If you don't have a threat intelligence program in place, the one easy bit of advice I'd offer to keep up to date is to subscribe to alerts from your country's CERT. For the U.S., <https://us-cert.cisa.gov/ncas/alerts> is a good example.

***TAG Cyber: What are the top use cases for ThreatQ TDR Orchestrator?***

**THREATQUOTIENT:** While we're passionate about automating as much as we can, with ThreatQ TDR Orchestrator we're focusing on specific use cases in the area of detection and response.

- Evidence gathering: Has some event occurred that you need to gather additional information before a determination is made on how to handle it? Well, let's automate that across your existing tools, and in addition to gathering that information, ThreatQ will consume it for analysis and prioritization as well.
- Targeted automated enrichment of data: As we just discussed earlier, too much data can be a bad thing, so why waste your enrichment API tokens and make the situation worse with more irrelevant events and data? Being able to control when an enrichment takes place based on existing knowledge about the object should bring big improvements to this pipeline and process.
- To accelerate a user's ability to automatically update and manage threat data: This is, of course, a function that ThreatQ has performed really well for a long time. But, with the new TDR ability to trigger specific updates, we have created a new approach users can take to ensure information is more accurate and delivered in a timely manner.







Tohmo

AN INTERVIEW WITH JESPER TOHMO,  
CTO & CO-FOUNDER,  
AND



Link

ZACK LINK, SENIOR SECURITY ENGINEER,  
SHARDSECURE

# RENDERING DATA AT REST INCOMPLETE AND UNINTELLIGIBLE TO THREAT ACTORS

The use of public cloud infrastructure for sensitive data storage and processing is no longer considered the substantial business risk it was a decade ago. Due to advancements in cloud access management, cloud infrastructure entitlement management, and other like cloud-native controls, the risk of unauthorized cloud data access is not significantly greater than data risk in other environments. However, most cloud security technologies focus on protecting “front door” access, that is, how an end user would access cloud data.

Though front-end access is the low-hanging fruit of cloud data security, none of these technologies prevent back-end administrative access to sensitive data – arguably the most damaging kind of access if exploited by a malicious user. Traditional security advice says security teams should simply tighten admin access controls, but ShardSecure takes a different approach. The company’s microsharding technology is designed to address the cyber risks of back-end access to data hosted in cloud infrastructure. CTO and Co-founder Jesper Tohmo and Senior Security Engineer Zack Link of ShardSecure explain microsharding and its value proposition.

**TAG Cyber:** *In previous TAG Cyber publications, you’ve explained that microsharding breaks up data into multiple components that are separated, obfuscated, and stored across disparate cloud infrastructure. What is the business benefit?*

**SHARDSECURE:** Cloud service provider infrastructure is public by nature, built for ease of access and speedy deployment. The resulting CapEx reductions, deployment speeds, and on-demand pricing provide appealing business benefits in terms of infrastructure saving and speed to market. However, a storage bucket left open on public cloud infrastructure presents a big cyber risk.

Public data exposure can present immediate security fallout, or perhaps worse, malicious actors could be viewing data before IT stakeholders are aware of the breach. Microshard™ technology shreds data into fragments that can be as small as single digit bytes to eliminate data sensitivity, mixes and pollutes it with false shards to completely remove all data value in the storage area, then distributes shards to multiple cloud locations to ensure data is incomplete. This helps clients avoid costly breach expenses and can even



reduce compliance burden by reducing what is in scope as sensitive data. Importantly, microsharding provides a way for organizations to embrace the agility and flexibility of public cloud without fear of a breach.

***TAG Cyber: Can you please explain the algorithmic strategy for these processes?***

**SHARDSECURE:** Microshard technology involves a shred, mix, and distribute approach to provide defense in depth for data at rest.

First, data is shredded to reduce its sensitivity. While legacy sharding methods, used primarily to improve performance, involve splitting files or volumes into multiple pieces that are a few thousand to a few million bytes in size, ShardSecure's technology breaks data into extremely tiny fragments too small to be valuable to malicious actors. A single kilobyte fragment is large enough to contain III Social Security Numbers, but microshards can be as small as four bytes, far too small to contain any sensitivity.

Next, data is mixed to eliminate any data value. Multiple microshard containers are created equal to the number of configured storage destinations, and poison data is added to increase complexity. Microshard containers do not retain file headers, names, extensions, or location data. Microshard storage areas contain no information about the type of data stored, and as sensitivity has been eliminated through microsharding, malicious actors would have no way to derive meaning from the data they've accessed.

Finally, data is distributed to multiple storage locations that can include multiple cloud providers and/or on-premises locations. Microshard locations are completely unaware of each other. This ensures that data will always remain incomplete and unintelligible in any single storage location, unlike legacy security solutions such as encryption with which compromised data is complete and can technically be unscrambled.

***TAG Cyber: How does microsharding complement front-end cloud-based security technologies?***

**SHARDSECURE:** ShardSecure helps secure data on back-end cloud infrastructure where privileged cloud administrators perform important daily activities including patch management, software updates, and other critical tasks that bear serious consequences in the event of data breaches.

Even if encryption is used on the front end, application servers and cloud admins often have access to the keys. Whereas legacy solutions have provided little in the way of back-end cloud data security, microsharding separates sensitive data from privileged

If data has been shredded to the extent that a bad actor is unable to extract even a credit card number or Social Security Number, it can be argued that the data is no longer classed as “sensitive.”

administrators who could be compromised, disgruntled, or simply make mistakes that cause data breaches. Microsharding can help enterprises achieve zero trust in data security.

Microsharding reduces the attack surface of applications in the cloud and the entire data storage area (gigabytes to petabytes) to the small attack surface of the microshard engine, pointers, host map file, and applications (mere megabytes). If attackers breach a cloud administrator’s account for one cloud provider, the microsharded data on that cloud provider cannot be used to reconstruct any files or even a small amount of sensitive information. If attackers breached all the enterprise’s cloud storage, the microsharded data could not be reassembled without access to the microshard engine, pointers, and host map file.

***TAG Cyber: How prevalent are back-end exploits?***

**SHARDSECURE:** While a solid 30% of data breaches are intentionally caused by internal actors,<sup>1</sup> an overwhelming majority of damaging cyber security events can be traced back to the impacted organization in some way — most commonly to a misconfiguration. In fact, in 2018 and 2019 alone, over 33 billion records were left exposed in the public cloud.<sup>2</sup>

Exposed public cloud storage buckets have yielded catastrophic consequences. The Ponemon Institute estimated that exposed records in 2018 and 2019 cost companies \$5 trillion. As the 2020 Data Breach Investigations Report cited that 70% of all breaches involve outside actors, it’s clear that legacy cyber security solutions alone are insufficient in the age of cloud.

***TAG Cyber: How does microsharding help with security and privacy compliance mandates?***

**SHARDSECURE:** ShardSecure eliminates data sensitivity such that it improves regulatory compliance. Regulations such as GDPR, HIPAA, CCPA, CPRA, and PCI DSS can be costly to comply with and expensive if their standards are not upheld. However, if data has been shredded to the extent that a bad actor is unable to extract even a credit card number or Social Security Number, it can be argued that the data is no longer classed as “sensitive,” dramatically reducing companies’ data protection burden and the cost of compliance. For example, if the cloud storage administrator account is attacked — a common concern in complying with regulations such as GDPR — data that has been microsharded is not in jeopardy.

Microsharding can reduce the scope of storage locations that must comply and scope of audits for those environments. For instance, the cloud storage locations that store the disparate microshards might no longer have to comply with GDPR — none of them contain any data that would be considered sensitive.

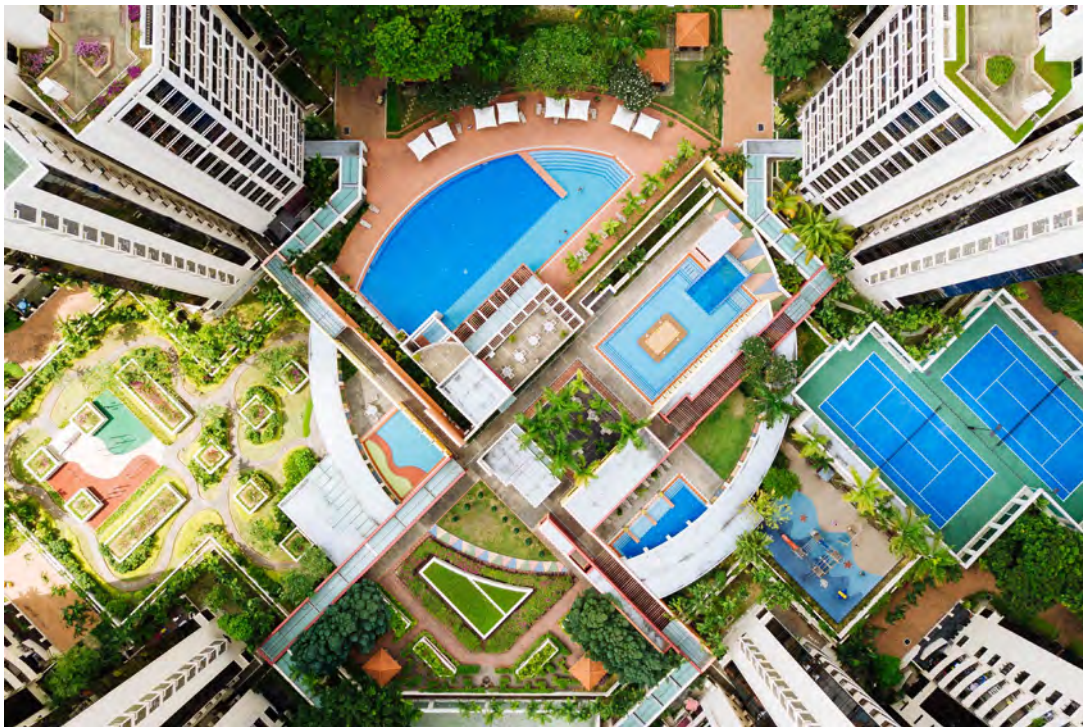


Of course, the applications that use the data reconstructed by ShardSecure from the microshards would still be in scope.

By virtue of eliminating the sensitivity of data, microsharding makes it easier for organizations to store larger quantities of data for longer, without multiplying the attack surface or increasing risk along with data quantities. This includes the long-term security of storage backups, an often-neglected category of data. Organizations can confidently store large volumes of microsharded data on-premises or in the cloud, thereby improving audit outcomes and helping ensure compliance.

<sup>1</sup> 2020 Data Breach Investigations Report, Verizon

<sup>2</sup> 2020 Cloud Misconfigurations Report, DivvyCloud





Di Bello

ANTHONY DI BELLO,  
VP STRATEGIC DEVELOPMENT,  
AND



Munusamy

RAJ MUNUSAMY, SR. DIRECTOR, SECURITY  
PRODUCT MARKETING, OPENTEXT

# A FORENSIC APPROACH TO RANSOMWARE PREVENTION

Ransomware is a persistent cyber problem without an end in sight. Conventional security advice says that to prevent ransomware, users should not click on links or open attachments from unknown senders. But attackers never make it that easy. Bad actors craft convincing emails that can deceive even the most discerning eye.

To land in users' inboxes, ransomware first needs to get through an endpoint. Savvy security vendors are therefore focusing efforts on detecting anomalies at the endpoint – before a user has the chance to make a mistake or is tricked— thereby preventing a click or a download and subsequent data breaches and costly disruptions to business operations.

OpenText is taking a forensic approach to ransomware prevention. The company's EnCase Endpoint Security product establishes baseline behavior at each endpoint, uses the baselines to detect anomalies, then configures policies to prevent ransomware detonation. Recently we spoke with Anthony Di Bello, VP Strategic Development, and Raj Munusamy, Sr. Director, Security Product Marketing, at OpenText about ransomware and how they're helping customers avoid endpoint-based breaches.

***TAG Cyber: With all the endpoint security products on the market, why are ransomware and conventional malware still so successful?***

**OPENTEXT:** Ransomware attacks increased by about 500% during the pandemic, with recent attacks on Colonial Pipeline, the Irish Health Services, and JBS capturing global media headlines. In many cases, these ransomware attacks are not sophisticated. They leverage weaknesses in network firewalls, lack of multi-factor authentication, and the ease with which documents can be corrupted with malware. It all boils down to the security awareness and readiness of organizations.

***Here are three ways to strengthen defense against ransomware and traditional malware attacks.***

- Ensure optimal security awareness: Security awareness training is mandatory. People are often the weakest link in an organization's defense system. But this can be fixed through the efficient delivery of relevant knowledge on subjects including information security, social engineering, malware, and industry-specific compliance. This increases employee resilience to cyber attacks at home, on the move, and at the office.

- Embrace a defense-in-depth (DiD) approach: With DiD, security solutions are deployed throughout the network, creating layers to threat detection and risk mitigation. Multiple tools contribute to threat identification, ensuring that if one layer fails to detect a threat it will be caught by another. But these tools often aren't designed to work together, resulting in alert fatigue and delays in detection and response. DiD implementations require deep integration. For this purpose, an API-first strategy is recommended in selecting security products that form the multiple layers of a DiD architecture.
- Assume you have been breached; keep hunting: Threat hunting is an essential component in today's cyber security strategy. Continuous threat hunting delivers preventative support that identifies the existence of threats and malicious activity across the cyber kill chain. Also, use a threat hunting service that leverages world-class threat intelligence. This enables faster remediation and recommendations to close gaps in security protocols and policies.

***TAG Cyber: What signals should an effective endpoint security product be collecting to detect and prevent ransomware from executing?***

**OPENTEXT:** It is a misconception to assume collection is required for the detection of threats at the endpoint, although some solutions require this. The question is: What signals should an effective endpoint security product have visibility into?

Effective endpoint threat detection requires unfettered access to disk, memory, and registry to ensure access to the necessary signals and to correlate signals to deliver higher fidelity alerts. To achieve unfettered access, the product needs the ability to forensically parse the file system independently of the resident operating system (OS). This is critical, as attackers can easily hide activity from the resident OS. Kernel-level rootkits are a great example.


For specific signals, the product should have access to event logs, scheduled tasks, connection information, files (including open files), registry, threads, drivers, handles, DLLs, processes, and OS management instrumentation data such as Windows WMI, at minimum. It should also have access to any metadata associated with these signals. While there are additional signals accessible by OpenText's EnCase Endpoint Security, the above is a good starting list.

***TAG Cyber: Why does OpenText focus on YARA rules and STIX as the top IoCs in endpoint detection?***

**OPENTEXT:** While EnCase Endpoint Security does support YARA and STIX-based scans, its detections are crafted around the tools,



**Effective endpoint threat detection requires unfettered access to disk, memory, and registry to ensure access to the necessary signals and to correlate signals to deliver higher fidelity alerts.**



tactics, and procedures (TTPs) associated with malicious network activity. While IoCs can be helpful, they reflect static information such as known bad hashes, IP addresses, filenames etc., and are easily defeated as attackers vary their signatures for this very reason.

EnCase Endpoint Security TTP-based detections consider a variety of actions in sum to detect potential compromise. They are not looking for static matches, but rather the types of activity associated with an attacker or insider operating maliciously within the network.

A simple IoC for PowerShell, for example, would generate countless false positives and force analysts to perform a manual investigation into how any given instance was launched. A TTP-based detection, on the other hand, ensures only truly suspicious instances of PowerShell are alerted upon.

***TAG Cyber: How do OpenText's history and legacy products shape your endpoint security platform?***

**OPENTEXT:** OpenText has been developing deep expertise and solutions in information management over 30 years. This includes the acquisition of Guidance Software and Carbonite to form our Security & Protection Cloud. EnCase Endpoint Security is a core product in our security portfolio. It is built on Guidance's 25-year leadership in digital forensics. EnCase Endpoint Security today not only offers deep forensic parsing capabilities through its agent that operates at the kernel level, but also is fully aligned to the MITRE ATT&CK framework. In the most recent MITRE Round Three Evaluation, EnCase Endpoint Security came out tops in Real-time Detection, Visibility and Flexibility. The product has robust DFIR capabilities.

In addition, EnCase Endpoint Security also comes embedded with Webroot Brightcloud® Threat Intelligence, an OpenText security service. Among others, this allows EnCase customers to benefit from the product's web classification and reputation services, ensuring users are protected from malicious websites.

***TAG Cyber: What are the new, stealthy phishing and social engineering tactics attackers are using to fool users? It's not the "Nigerian Prince" emails that are a threat today.***

**OPENTEXT:** The 2021 Webroot Brightcloud® Threat Report showed that 86% of malware is unique to a single PC. Further, the study also found that of the endpoints that get infected, more than half will get infected more than once. This highlights the need for world-class protection, detection, and response capabilities covering all endpoints across the enterprise.

Industries with the highest infection rates include wholesale trade (attacks +32.2% over average), mining/oil/gas (+32.0%), manufacturing (+25.9%), public administration (+25.0%), and information (+22.1%).

Ransomware is gaining notoriety. As Kelvin Murray, OpenText's Senior Threat Research Analyst says: "In most cases, ransomware isn't the beginning of a compromise. It's the end state, where criminals cash in after an extended period. By the time you realize you've got ransomware on your network, the criminals may have been in there, watching, listening, and tampering with things for weeks or months without your knowledge. They might've even checked out your financials, so they know what kind of ransom to demand."





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

## REDUCE YOUR MTTD AND MTTR WITH CYBER RANGE TRAINING

“Even the best sports teams need to practice.” That is the motto posted on the Cloud Range homepage. Cloud Range, a provider of secure, cloud-based cyber range training, is helping security operations teams keep their skills honed and their ability to detect and defend against real-life cyber threats sharp.

It wouldn't be crazy to think that SOC analysts and incident responders already get enough on-the-job training. As companies' digital ecosystems sprawl, and cyber attackers grow more skilled and slicker by the day, SecOps teams have plenty of work on their hands, from monitoring and triaging alerts, to investigating suspicious activities and preventing them from causing an incident, to stopping an incident in progress.

But just like a major league baseball team must practice frequently and review footage between games, SecOps teams need to practice outside live environments. TAG Cyber recently spoke with Debbie Gordon, Founder & CEO of Cloud Range, about why range training is important and how it helps both employees and businesses.

**TAG Cyber: What are the main differences between a live environment (i.e., on-the-job experience) and a cyber range?**

**CLOUD RANGE:** Simply put, time is money. Figuring things out as they are happening is not only inefficient, it is simply irresponsible. Security leaders must be proactive in ensuring that their security operations teams have the ability to detect, investigate, and respond to threats in a methodical way, even amongst apparent chaos.

This is done using immersive simulation. When given the opportunity to work in a safe, protected environment, members of security teams make better decisions and are not afraid that they will take the company down with one wrong move. Conversely, if people have to depend on “on-the-job” training, they may be more hesitant to take action, for the fear of making a mistake. This is something we see constantly. With proper communication and collaboration, people are able to make better decisions using simulation on a cyber range, be more confident, and ultimately have a better outcome.


Once this translates into a live environment, security teams are more prepared, there is less chaos, and the end result is a faster and more effective response.

**TAG Cyber: Are you seeing an increase in interest for cyber range training? Why?**

**CLOUD RANGE:** In just the past 3 years, there has been a drastic increase in the market's understanding and adoption of cyber ranges. Lately, we are seeing companies proactively allocate budget toward implementing cyber range programs in their organizations. In just a



Figuring things out as they are happening is not only inefficient, it is simply irresponsible.



few short years, our conversations with CIOs and CISOs evolved from explaining the purpose and value of a cyber range to helping leading organizations successfully implement a cyber range program in their organization. It is no longer a “nice to have;” it is a “must have,” now that the technology and solutions are so flexible and customizable. Today, more security leaders understand that simulation training has become a standard in organizations’ security programs.

If you think about other categories of “life safety,” i.e., medicine, law enforcement, firefighting, etc., they all require simulation training. Cyber security is the only life safety category that does not (currently) require simulation training. However, this is quickly changing, as leading organizations are realizing how important it is to train the people defending their companies by using simulation so that they are ready to react quickly and efficiently – having practiced defending using simulated cyber attacks in a live, contained environment. This creates muscle memory and situational awareness that is imperative for ensuring teams are prepared for the unexpected.

***TAG Cyber: What types of companies or individuals are showing interest in cyber range training?***

**CLOUD RANGE:** Our customers include primarily enterprise/F1000 security teams from industries including banking/financial services, healthcare, consulting, retail, logistics, and more. Additionally, state governments, military, and higher education are also utilizing Cloud Range’s services.

Finally, we are seeing tremendous growth in the critical infrastructure sector/OT/ICS arena. Preparedness/training is such a big area of focus for that market, not only because of the obvious threats that we are seeing in the news, but also because there is a lot of disparity in organizations between IT and OT, which makes their risk even greater. By incorporating simulation training into their organizations, they are able to ensure their teams can proactively prepare for events, and also help with the necessary convergence of the IT and OT parts of the business.

***TAG Cyber: How does this help if the attackers are practicing, too?***

**CLOUD RANGE:** The cyber security space is dynamic. What your security team knew yesterday is not what the hackers will know (and use against you) tomorrow. The fact that attackers are constantly coming up with new threats is all the more reason for security teams to engage in continuous simulation training. As the threat landscape increases, it’s important, now more than ever, that security teams have up-to-date skills to detect, defend against, and remediate the most advanced attacks.

Cloud Range utilizes the MITRE ATT&CK framework to design attack scenarios that reflect adversary tactics and techniques. Our customers have the privilege of not just reading about these, but are able to be immersed in these live attack scenarios to ensure that they know what to do, and more importantly, how to detect and respond to these tactics and techniques, which are ever-changing.

The more a security team practices defending against a variety of threats, the more skills they will develop and hone, including critical thinking skills that can be applied to any type of attack, whether it's an attack they have experienced before or not. Continuous simulation exercises and training give security teams the opportunity to practice together and develop a rhythm and skills that they can use and depend on in a split second when an attack occurs.

***TAG Cyber: What measurable results can SOC analysts, incident responders, and their employers expect from cyber range training?***

**CLOUD RANGE:** Without proper metrics, it's hard to know how prepared a security team is for an attack. It is imperative that security leaders are able to see measurable improvements in their mean time to detect (MTTD) and mean time to respond (MTTR). The ability to obtain objective, measurable results from simulation exercises becomes imperative in assessing the actual level of preparedness of a security team versus simply hoping they will do what is necessary as quickly and efficiently as possible.

Cloud Range has developed a proprietary assessment model that measures both team performance as well as the performance of the individuals that make up the team. This gives leaders the intelligence that they need to be confident that their teams are getting the skills and experience they need, which is ultimately measured in their ability to improve on MTTD and MTTR.

Additionally, Cloud Range's assessment system maps results to the NICE Framework, including multiple measurements of knowledge, skills, and abilities (KSAs). These results capture a team's progress over the course of a program and show exactly where a team's and its individuals' strengths and weaknesses are.

Finally, in addition to technical skills, participants are also measured on soft skills, including communication and collaboration, which are imperative in cyber security-related events.



AN INTERVIEW WITH CRANE HASSOLD,  
SENIOR DIRECTOR OF THREAT RESEARCH, AGARI

## MODEL “GOOD,” NORMAL BEHAVIOR TO PREVENT PHISHING AND BUSINESS EMAIL COMPROMISE

Despite the myriad communications platforms available to businesses and individuals, email remains the core method and mechanism of communication. According to a McKinsey analysis, the average professional spends nearly 30% of their day reading and responding to emails, receives 120 emails per day, and yet is left with piles of emails unread and un-responded to. The overabundance of email traffic coupled with typical business busyness is a recipe for cyber disaster. And cyber criminals take note.

Email is the primary vector for social engineering attacks and business email compromise (BEC). Threat actors have grown savvy over the years, crafting emails that look and feel like a legitimate email – often conducting in-depth research on high-profile targets so their communications seamlessly blend in. The reason email compromise proliferates is because it works. Agari, a trusted identity email provider, helps companies stop phishing and BEC attacks. Crane Hassold, Senior Director of Threat Research at Agari, spoke with TAG Cyber about some of the challenges in email security.

**TAG Cyber:** *Phishing and business email compromise are old tactics by this point. What are some of the new techniques threat actors are adopting?*


**AGARI:** While BEC attacks have increased significantly in volume since around 2015, some newer types of more impactful BEC attacks have become increasingly common in recent years. For example, vendor email compromise (VEC) attacks – hybrids of credential phishing and identity deception attacks – are some of the most impactful cyber threats businesses face today. In these attacks, cyber criminals first compromise the mailbox of a high-value target employee that has access to payment information. They then collect intelligence from the mailbox over a period of time – weeks or months – and use the intelligence to inject themselves into an existing payment process with a customer. The result is that they are able to redirect the payment using an extremely realistic-looking email. Other variations of VEC attacks, such as requests for financial aging reports, have recently put a spotlight on the role of third-party suppliers as a significant target for cyber criminals.

**TAG Cyber:** *What is the scope of the business email compromise reach?*

**AGARI:** One of the unique challenges with business email compromise is that it impacts businesses all around the world, regardless of size or location. We consider BEC attacks to be industry-agnostic because these cyber criminals are simply trying to identify employees with access to money, regardless of the sector they're in. And while gift cards have become the primary payment method requested by BEC actors in



**We consider BEC attacks to be industry-agnostic because these cyber criminals are simply trying to identify employees with access to money, regardless of the sector they're in.**



what might be seen as very basic types of attacks, it opens up the possibility for any employee at a company to be targeted by one of these scams.

***TAG Cyber: How is Agari incorporating data science into your platform?***

**AGARI:** Agari has a huge data set from our work with businesses and visibility into trillions of emails every year. We use machine learn to analyze the content of these emails and correlate results, drawing meaningful and actionable conclusions; machine learning is central to how Agari solutions help an organization protect itself from phishing attacks.

Our data science looks at everything from sender identity to geolocation, time of day, recipients, subject lines, attachments, URLs, and more to assess whether an email is fraudulent or genuine, whether it presents a risk, etc. That model assigns a trust score to every incoming message, triggering a variety of defensive actions as a result.

***TAG Cyber: Why is this important and what benefits does it reap?***

**AGARI:** We look at it this way: traditional cyber defenses are a little bit like the old adage about generals always fighting the last war. You can create a rule set that is a mile high or a feed of threat indicators millions of items deep but still miss the next new, novel attack. Instead, the Agari approach models all the normal, good behavior that's typical of a customer's organization in order to identify anomalies that have a high likelihood of being a threat. It's the only way to effectively stop the identity-based deception that drives phishing and business email compromise.

***TAG Cyber: One of the differentiators for Agari is your threat research team. Tell us a little about what they do and why.***

**AGARI:** The Agari Cyber Intelligence Division (ACID) is the only intelligence team dedicated to researching BEC attacks on a daily basis. The team utilizes active defense techniques that provide in-depth insights into the full BEC attack cycle, allowing us to better understand what happens after an attack is successful and learn more about how a BEC actor's tactics evolve over time. We're able to feed this intelligence back into our email defense products, as well as work with industry partners and law enforcement to impact the threat posed by BEC from multiple angles.



KARIM HIJAZI,  
CEO AND FOUNDER, PREVAILION

# USING COMPROMISE INTELLIGENCE TO PREVENT CYBER ATTACK

Cyber security experts talk about the “attack surface” and the need to understand it to protect it. However, often, enterprises are so overwhelmed by what’s going on on their networks and with their 3rd party providers that they don’t or can’t look further down the supply chain. While resourced companies *do* conduct external scans, basic scanning is not enough to detect active compromise. Further, scanning can create “noise” that makes it hard to understand where the real problems are.

Instead, enterprises need compromise intelligence: continuous monitoring of attacks against a company’s infrastructure *and* their supply chain. One look at the mega breaches of the last decade tells you everything you need to know about understanding and protecting the supply chain.

Prevailion is changing the definition of “attack surface.” We recently spoke with Karim Hijazi, CEO and Founder at Prevailion, about why companies need to look beyond their borders — and in a new way — to create true attack surface awareness that leads to action.

***TAG Cyber: With all the scanning and security tools commercially available, why is supply chain attack surface management still so hard?***

**PREVAILION:** The majority of scanning tools are meant to provide security teams with an understanding of their potential risks and security gaps that could lead to a compromise by a threat actor. However, these tools all simply provide prioritization or scoring to address the “highest risks” or worrisome gaps. This is helpful for the purposes of where to address “your walls” or the strength of your supply chain partners’ “walls.” However, whether the cause is phishing or another attack method, attackers know how to bypass these walls and compromise companies’ infrastructures.


A risk score does not tell the “parent” organization if their partner (a.k.a., a third party) is actively compromised, thus putting the parent at a much higher actual risk versus potential risk. So for instance, if I know my supply chain partner’s attack surface has been compromised, I can take more meaningful action to protect myself.

We’ve already seen XDR and endpoint platforms take too long to piece together noisy indicators of compromise, thereby preventing cyber security teams from getting in front of and thus avoiding an attack. These teams need actionable evidence of compromise — in advance of an attack — that only compromise intelligence delivers.

***TAG Cyber: How are attackers using the vastness and ephemerality of the open internet to executive hard-to-detect attacks?***

**PREVAILION:** Attackers must leverage the open internet to navigate and communicate to and from a target organization they’ve compromised

DNS providers globally are the “transfer stations” that make the internet work but are not meant to have visibility into the messages and “cargo” being moved through internet communications.



or want to compromise. This is typically referred to as “command and control” or “C2” activity by which attackers gain remote access to a system, control the spread of an infection, download more malware, exchange ransomware keys, steal data, and even control and monitor how well ransomware is working.

An internet provider is hard-pressed to know whether these communications are being used for malicious purposes by threat actors. Rather than simply monitor the dark web or chat rooms for already stolen data or poor fidelity indicators of compromise, companies can leverage counterintelligence to find suspicious communications, analyze it for malware, and then work with providers to “convict” domains associated with C2 activity. It’s this ability to proactively hunt down attacker communications, quickly perform counterintelligence, and report the findings back to an already compromised organization that can provide the early warning needed to prevent the detonation and subsequent damage that so many other solutions are unable to achieve.

***TAG Cyber: We’ve been hearing a lot more lately on the need to monitor and log DNS. Why?***

**PREVAILION:** DNS is one of the key anonymous mechanisms that attackers use to secretly route their malicious communications. DNS providers globally are the “transfer stations” that make the internet work but are not meant to have visibility into the messages and “cargo” being moved through internet communications. However, working with compromise intelligence, organizations can map compromises that have penetrated their walls from the outside and understand which resources are impacted internally; this is critically faster identification and remediation. Once again, the goal is to get ahead of the attacker who has already gained entry into the kingdom.

***TAG Cyber: Briefly describe Prevailion’s APEX™ solution.***

**PREVAILION:** Prevailion’s APEX is a SaaS cloud-based platform for security teams’ real-time monitoring of their organization for compromises as well as monitoring their supply chain partners. APEX is a real-time platform that is zero touch and does not use agents or have any deployment requirements. Yet, it can significantly impact an organization’s security stack and overall program by offering up early evidence of compromise that tells the user not only the IP address and malware family, but also has the potential to reveal the threat actor group and/or origin of the attack. It is a combination of the specialized counterintelligence, incomparable provider partnerships, and proprietary software analytics built into the platform that allows APEX to monitor for and detect compromises globally. This same approach also enables compromise intelligence on a company’s supply chain partners.



***TAG Cyber: How would companies use a platform like Prevaillon's?***

**PREVAILION:** The primary use case for Prevaillon's compromise intelligence is giving a company those early warnings, accompanied by actionable data on compromises that customers can use to act on threats before the threats are detonated and the threat actor is either able to steal data or execute ransomware. Our solution is a critical piece of breach mitigation for companies' security operations monitoring programs.

In addition, our customers commonly use our solution to monitor their supply chain partners to determine their downstream risk. They then use that intelligence to work with partners and improve the security of both companies. Supply chain attacks have been very popular with attackers and have done immense damage to organizations globally. Prevaillon provides the ability to move beyond just potential risk to finding active compromises in real time, keeping companies continuously ahead of attackers.

The core of the value we offer is for compromises that have remained undiscovered by XDR or SIEM or are too early in the attack chain to detect by those solutions. We are able to provide high-fidelity evidence (virtually no false positives) of compromised assets in customers' environment (or that of a partner) which drastically reduces mean time to detection (MTTD) and as a result, mean time to respond (MTTR).





AN INTERVIEW WITH ANJAN VENKATRAMANI,  
CEO AND CO-FOUNDER, PRISMO SYSTEMS

## CONTINUOUS ASSESSMENT AND CONTROL FOR CYBER RISK MANAGEMENT

Cyber security is a complex amalgamation of people, processes, and technologies (PPTs) that combat enterprise cyber risk. As businesses have become predominantly digital and significantly interconnected, the attack surface has sprawled, causing a corresponding increase in the ways and places cyber practitioners must look at their PPTs to prevent and mitigate cyber threats.

Today, the average organization has more than 75+ security point products deployed to help them in such endeavors. Some of these tools (still) require manual management, and many of them don't integrate to offer security practitioners a streamlined, meaningful way to manage cyber risk. Years ago, security information and events management (SIEM) technology was developed to create a centralized logging system that would remedy the problem. But today, even next-gen SIEMs have blind spots.

Prismo Systems was founded to eliminate security blind spots and missing technology integration. Recently, Anjan Venkatramani, CEO and Co-founder, spoke with TAG Cyber about Active Cyber Risk Management, what it means, and how it differs.


**TAG Cyber:** *Can you explain what Active Cyber Risk Management is and how it helps customers?*

**PRISMO SYSTEMS:** Active Cyber Risk Management (ACRM) is the approach and philosophy that Prismo prescribes for enterprises to continuously assess, control, and contain their overall cyber risk and assure compliance with frameworks such as NIST, MITRE, OWASP, etc.

As organizations have become perimeter-less, with distributed workforces and hybrid-cloud deployments, the security exposure surface has grown geometrically and exceeded the capabilities of today's siloed security solutions. Prismo quantifies the exposure in terms of two kinds of risks — imminent risk and inherent risk. Imminent risk stems from an activity, such as malware that is actively triggering, while inherent risk stems from missing controls, such as a software vulnerability that could be exploited. Both types of risk, if unaddressed, can escalate to data breaches, loss of service, compliance fines, and ransom demands, among others.

In contrast to today's approaches, ACRM embodies the principles of NIST zero trust: "Trust nothing, authorize continuously, and protect all resources wherever they are located." The objective is to secure the entire security exposure surface from external attacks, but just as importantly, internal exposures due to human errors or configuration drift. ACRM systematically and proactively addresses the majority of, if not all, risks through the discovery of granular context, application of deep learning, accumulation of risk scores over time, and across all platforms, automation of responses where effective, and

Because these attacks utilize low-impact and discrete intrusions over a significant period of time, the signals typically get lost in a sea of alerts.



enablement of custom responses to adapt to the organization's specific needs.

***TAG Cyber: Why is ACRM necessary? What are tools like SIEM, SOAR, and XDR missing that ACRM can achieve?***

**PRISMO SYSTEMS:** To highlight why an ACRM approach is critical, let's look at the supply chain attacks that have been in the news recently. These attacks account for an estimated two thirds of breaches across all industries, including government and defense. So, countering supply chain attacks is critical. Because these attacks utilize low-impact and discrete intrusions over a significant period of time, the signals typically get lost in a sea of alerts. Further, the signals are not linked into an attack by a SIEM, SOAR, or XDR until typically after a breach occurs – and that's too late.

Prismo continuously assesses risk according to NIST, MITRE, and OWASP frameworks, and consequently, even the most subtle, discrete, and long-term intrusion is detected, prioritized, and automatically mitigated by an active response. That way, even successful and independent compromises are neutralized before damage occurs. That's a real-world embodiment of the principles of zero trust.

***TAG Cyber: What are the top complaints you hear from SOC analysts about current data collection and correlation tools and processes?***

**PRISMO SYSTEMS:** SOC analyst feedback is aligned with my own experience in a SOC. It takes literally months of effort to research a successful intrusion, map it to a framework such as NIST, and build a kill chain. By then the damage is done and the threat actor is long gone. Further, the threat actor is already leveraging new tactics to compromise the environment again. So, SOC analysts tell us that current data collection and correlation tools are simply being overwhelmed by today's attacks, forcing them to perform laborious, manual analysis.

***TAG Cyber: What is the Prismo Systems Transaction graph and how do customers use it?***

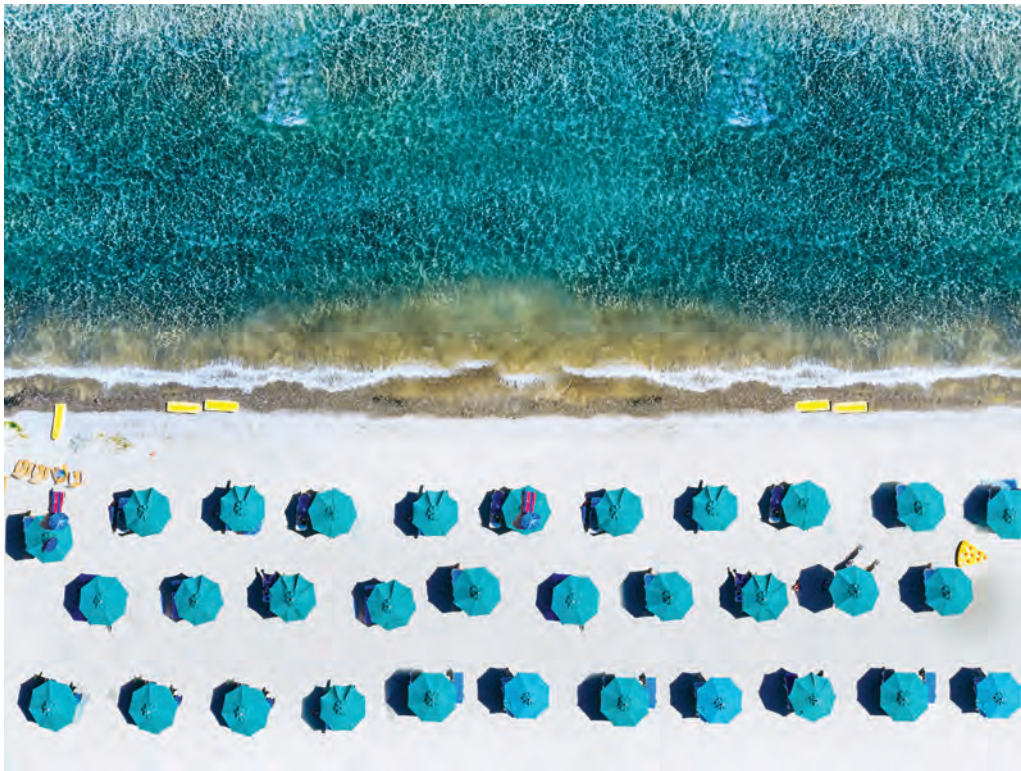
**PRISMO SYSTEMS:** The Prismo Transaction Graph is the core technology that powers our Active Cyber Risk Management platform. The Prismo platform enforces zero trust principles in real time, meaning that users, devices, applications, and APIs are treated as assets and their interactions with assets or data objects are authorized and secured. Authorization is continuous rather than once per session or connection, and based on Prismo's Dynamic Risk Profile. The dynamic risk profile is a unified, continuous, event-driven assessment of risk measured across the entire IT environment. Since it is based on a cumulative risk score,



the risk profile enables rapid, early detection and automated mitigation of low and slow multistage attacks (such as supply chain).

***TAG Cyber: What types of compliance or industry standards does your platform address?***

**PRISMO SYSTEMS:** Prismo is also revolutionizing the concept of compliance from manual, static, snapshot-in-time spreadsheets to continuous, real-time compliance with automatic tracking. Prismo maps to industry standard frameworks including NIST (multiple specifications), MITRE, and OWASP. We also enable the organization to define its own KPIs that we then continuously track. Dashboards are always current with up-to-the-event precision and accessible to anyone with credentials and a browser. With Prismo, all security stakeholders from analyst to auditor to CISO are in the loop with access to real-time reports and dashboards at their fingertips, improving communication and coordination from the SOC all the way to the boardroom.





AN INTERVIEW WITH AYAL YOGEV,  
CEO, ANJUNA

## CREATING A SECURE, CONFIDENTIAL CLOUD COMPUTING ENVIRONMENT

Unintentional data exposure is a key concern for organizations that embrace public cloud infrastructure. While the environment, itself (when provided by a reputable player), may be secure, access controls and data management are the responsibility of the user/tenant. And several recent high-profile breaches have demonstrated why secure configuration and management must be top of organizations' lists, yet just how difficult and tricky they can be.

The risk of exploit that accompanies cloud usage extends to insiders and outsiders — users from the tenant organization, those from the provider organization, and third-party malicious actors. Thus, the risk equation increases exponentially; organizations need a better way to secure their data.

Cloud vendors have created their own “confidential clouds” that enable organizations to protect data at rest and in use. We recently spoke with Ayal Yogev, CEO at Anjuna, about secure enclaves, the confidential cloud, and how organizations can establish a more secure, comprehensive protection program for all data — including applications, algorithms, and cryptographic keys — throughout the data lifecycle.

**TAG Cyber:** *First, can you explain the concept of a “confidential cloud”?*

**AJUNA:** The confidential cloud is a secure, confidential computing environment formed over one or more public cloud providers. Applications, data, and workloads within a confidential cloud are protected by a combination of hardware-grade encryption, memory isolation, and other services that assure workload, data, and platform integrity. Similar to network micro-segmentation, confidential clouds are isolated from all processes and users in a default zero trust posture across systems. Unlike micro-segmentation, the confidential cloud secures an entire IT environment, including compute, storage, and networking. This allows it to support a much broader set of applications.

Secure enclave technologies are a building block for the confidential cloud that create a trusted computing environment within an untrusted host. “Enclaved” workloads and data can be both cryptographically and physically isolated from external entities, resolving one of the most persistent, fundamental, and dangerous vulnerabilities in computing — the exposure of data in memory at the heart of every data breach. Data created in a secure enclave is encrypted and/or isolated by default, putting the data owner in full control of how, where, and when it can be used.

Secure enclaves are one of the building blocks to establish a multi-cloud construct called the confidential cloud — but there they are only one of several building blocks.

Few CIOs will be willing to lock every one of their most important applications to a single cloud vendor and confidential computing stack.

Secure enclave technologies, while flexible, generally require an application to be modified to leverage their proprietary security powers. In addition, creating a confidential cloud requires integration with a number of cloud-specific services. The confidential cloud is a vendor-neutral abstraction implemented over secure enclave and other cloud security technologies that, like host virtualization, can be used immediately by IT organizations without modifying applications or IT processes; confidential clouds operate invisibly as part of IT infrastructure unseen by IT processes or staff.

***TAG Cyber: What are some of the mistakes organizations make when approaching data security in public cloud environments?***

**AJUNA:** The biggest mistake organizations make is to assume that they are safe in the public cloud because they use the same legacy perimeter-based protection schemes they use on site. Ask a CISO. Most will tell you that the public cloud can't be rationally trusted to keep sensitive data and work confidential. Given enough time, a breach of some kind, even unintentional, is an eventuality. And it isn't just CISOs who know there are fundamental security holes in public (and private) clouds that make them easy pickings for bad actors; so does every public cloud provider. That's why virtually every one of them now offers confidential cloud technologies. As discussed previously, offering these is one thing; making them useable is another.

***TAG Cyber: What are common barriers or misconceptions about securing data in cloud environments?***

**AJUNA:** Useability is probably the biggest issue. Confidential cloud and secure enclave technologies are widely available on virtually every public service provider. But, at the same time, these technologies haven't crossed the proverbial "chasm" that would enable wide adoption by enterprise IT organizations. This is partially because both cloud vendors and the industry have focused only on securing memory and data in use, long the security Achilles heel of virtually every cloud host. Securing stored data and networked communications have been left to complex, point, multi-vendor technologies that must be integrated into applications separately. This isn't viable for organizations that have thousands of legacy and packaged applications which can't be modified. Few CIOs will be willing to lock every one of their most important applications to a single cloud vendor and confidential computing stack. And finally, use of these secure technologies must not require modifying the applications.

***TAG Cyber: Can you give us a brief overview of the Ajuna Confidential Cloud Platform?***

**AJUNA:** Anjuna Confidential Cloud platform software effortlessly enables enterprises to safely run even their most sensitive



workloads in the public cloud. Unlike complex perimeter security solutions that are easily breached by insiders and malicious code, Anjuna employs the strongest hardware-based secure computing technologies available to transform the public cloud into safest computing resource available anywhere. Anjuna Confidential Cloud software operates far below both users' and IT processes to deploy without disrupting the business, even as it virtually eliminates data attack surfaces, threats from insiders, bad actors and malicious software, and puts the business in exclusive control of their data. Anjuna software makes the public cloud the safest place for private computing.

***TAG Cyber: What types of companies are adopting this technology?***

Ajuna: Businesses and governments run on secrets to maintain competitive advantage. They are the typical fast adopters of effective security technologies – banks, financial institutions, retailers, and governments. Anjuna's partners are among the most security conscious enterprises in the world.





## AN INTERVIEW WITH DAVE FURNEAUX, CEO, VIRSEC

# PROTECTING HIGH-VALUE WORKLOAD FROM CYBER COMPROMISE

Cyber attacks are increasingly hitting companies more rapidly than ever before. The resulting damage impacts the direct targets of ransomware and the victims' customers and supply chains. Despite the workload being the backbone of the enterprise's software infrastructure, the workload's security remains underserved.

Current workload security providers fail to protect workloads comprehensively. An enterprise workload could be executing hundreds of processes, many of which may be running vulnerable code. SecOps must therefore not only keep patching the workload continuously, but also dedicate adequate system resources to ensure the workload functions optimally. Thus, an effective workload security solution must protect vulnerable code in real-time and be capable of deploying, operating, and scaling alongside the workload.

Virsec, a provider of application-aware workload protection, was founded on the premise that current workload protection models are inadequate and flawed. TAG Cyber recently spoke with Dave Furneaux, CEO, about why holes in technology and processes persist and how companies can be proactive without increasing security analysts' time and effort.

**TAG Cyber:** Please tell our readers about Virsec's founding story.


**VIRSEC:** We founded Virsec with the desire to protect workloads in real time from known and unknown attacks and without needing an army of security analysts.

The two previous generations of cyber protection technologies examined either pre-execution context (e.g., IPS, WAF, etc.) or post-execution context (e.g., EDR, HIPS, anti-virus). Neither approach has the precise security controls or visibility to defend against sophisticated runtime attacks. These technologies still focus mainly on the attacker's techniques exhibited by traffic patterns, payload, and behavior. Therefore, SecOps must know the essence of all potential attack patterns ahead of time, the lack of which places them in an asymmetric battle with zero ability to win. Attackers tend to overcome this "knowledge barrier" (if we want to call it that) to successfully execute the code of their choosing and succeed at their task.

Virsec® Security Platform™ (VSP) application-aware security controls overcome this knowledge barrier through deep runtime visibility, which facilitates exact, and real-time response to even the most sophisticated cyber attacks. Protection is engaged within microseconds, not minutes, hours, or days later.

The only way to achieve the required visibility is to map the code running on the workload to produce guardrails (or AppMaps™, as defined in 22 of our 50 patents) and prevent the processes from violating these AppMaps. If the workload

**You cannot protect just a subset of code on the workload and expect to block an attacker, as most solutions do. You must defend all code running on of the application workload.**



strays from the AppMaps, protection is applied immediately, thus preventing the attacker from dwelling in the workload.

Application-aware security controls within VSP are the only controls that provide the required real-time visibility and capabilities to act as the final layer of defense against sophisticated attacks that are otherwise undetectable to pre-execution and post-execution security controls. Without security controls offered in VSP, the workload's runtime will remain a black box that provides fertile ground for the attacker.

***TAG Cyber: We've seen the emergence of many workload point products in the last few years. Why does your team feel these are insufficient?***

**VIRSEC:** We believe that VSP is unique because it protects workloads from the inside without the need for prior knowledge, signatures, heuristics, etc., across the entire attackable surface. The key to all of this is our AppMap™ technology and lightweight architecture. Our product leverages machine learning to extract the application and network topology for deployment automation that scales. Light VSP sensors ensure that the impact on runtime performance on the workload is almost imperceptible. We have thought through all of the key enterprise needs around deployment, maintenance, operational, and integration into existing toolsets and environments. Competing controls rely heavily on probabilistic behavior models and outside information to raise alerts long after the attacker has successfully attacked the application workload. Beyond being unprepared to protect the workload in real time, competing solutions change the protected software itself (VSP does not). Furthermore, competing controls are hard to deploy, scale, and maintain in enterprise environments.

***TAG Cyber: When you say "full stack" protection, what do you mean?***

**VIRSEC:** A typical workload will execute a mix of interpreted code, compiled code, and perhaps malware as well. You cannot protect just a subset of code on the workload and expect to block an attacker, as most solutions do. You must defend all code running on of the application workload. Therefore, when we use the term "full-stack" protection, we mean that all code and software elements, whether interpreted or compiled, are protected by VSP. Further, VSP delivers a zero trust and zero dwell time approach that ensures no end user-provided content can turn into malicious interpreted code and not even one instruction of any malware can execute.

***TAG Cyber: What are the attacker trends, as they pertain to workloads, that companies should be concerned with?***

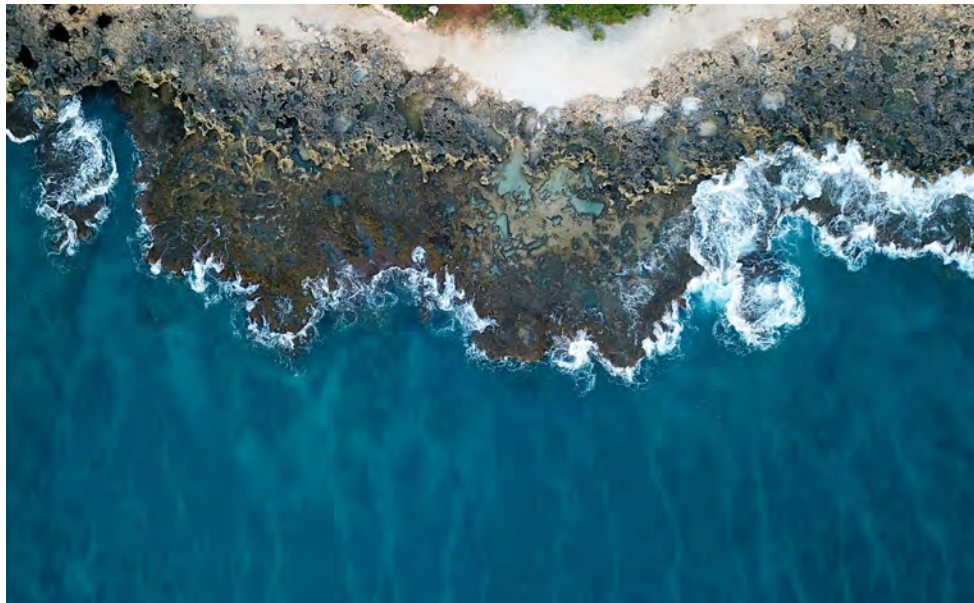
**VIRSEC:** As you know, nation-state perpetuated supply chain



attacks like the recent SolarWinds attack or ransomware attacks on critical infrastructure such as Colonial Pipeline and JBS are on the rise. In each case, the attacker infiltrated the network perimeter and targeted the workload's runtime. Organizations must absorb the fact that their security solutions must protect the workload's runtime in real time. VSP is leading this effort by focusing on protecting the application workloads at runtime.

***TAG Cyber: Several notable critical infrastructure breaches have occurred lately, and ransomware was involved in most. How does this, if at all, intersect with breach prevention and workload protection, which is not endpoint, user, or device focused?***

**VIRSEC:** There are many ways an attacker can breach the software infrastructure and proceed to unleash ransomware in the enterprise. Attackers look for the softest target they can breach, whether humans, code with an unpatched vulnerability, or code with some publicly undisclosed vulnerability. Penetrating a personal endpoint is not the final objective of a ransomware attack. Attacking a vulnerable application is the holy grail in a sense. An attacker is more likely to be successful if they impact the availability of a critical workload or extract confidential information from the workload. The enterprise is more likely to give in to the ransom when the attack affects a high-value workload rather than a personal endpoint.





## AN INTERVIEW WITH SAM CURRY, CHIEF SECURITY OFFICER AT CYBEREASON

# DEFENDING THE MODERN CORPORATE IT INFRASTRUCTURE WITH XDR

A utopian ideal for cyber security is preventing all compromises. In reality, attackers always find a way around even the sturdiest defenses. As a result, cyber detection and response capabilities have grown alongside the numerous prevention tools to become a core competency.

First there was network detection and response (NDR), then endpoint detection and response (EDR), and managed detection and response (MDR). Recently, application detection and response (ADR) has entered the nomenclature. Boiled down, what this ecosystem implies is that a holistic system for detection and response is needed. Thus, the emergence of eXtended detection and response or a convergence of the aforementioned categories, both equaling “XDR.”

Whatever you call it, SecOps teams need an integrated approach to incident handling. No SecOps team will exclude one of the above aspects from an investigation. Cybereason has expanded from its roots as an endpoint provider to offer more holistic services. Here, we speak with Sam Curry, Chief Security Officer at Cybereason, about the XDR market.

**TAG Cyber:** *In your words, what is XDR and what is its purpose?*


**CYBEREASON:** XDR is emerging as one of the best solutions for defending the modern corporate IT infrastructure against attacks, alongside popular solutions like SIEM, SOAR, and EDR, with which it must work. Done right, XDR does not pursue the job of collecting logs and all the noise out there but rather focuses on the telemetry most relevant to finding adversaries and understanding them, starting with behavioral data.

What EDR did for the enterprise, XDR does for the digitally transformed organization, extending to the cloud environments, identity plane, emerging endpoint type software-as-a-service and more. Five years ago the question of endpoint vs. network was the big discussion, and EDR emerged as the place to get the best telemetry, soonest, and most actionably. Now, EDR is being transformed in much the same way as the rest of IT, and XDR is the result. SIEM isn't going to make the stretch now after 20 years of getting it wrong, and in the end, if XDR does its job, cyber tasks will get better and CDR may even absorb SIEM and other adjacent functions and disrupt the older, more staid markets of the last two decades in much the way it has disrupted EPP.

**TAG Cyber:** *From a buying perspective, what are the “must haves” in an XDR platform?*

**CYBEREASON:** XDR must serve three key use cases for the extended enterprise as primary functions: finding advanced attacks such as RansomOps and supply chain attacks, enabling analysts to hunt for their own signals with queries they creatively come up with, and facilitating

**Predictability means that the opponent can seek to abuse the automation to hide or, worse, to their own ends.**



and accelerating ever more complete remediation. Secondary requirements include playing nice with existing tools like EDR, CWPP, EPP, SIEM, SOAR, and more, but also automating, facilitating forensics, enabling postmortem analysis, and doing as little harm as possible.

Perhaps the most exciting breakthrough — and becoming more and more of a necessity — is the notion of indicators of behavior (IoBs), good and bad. These are the recording and arrangement of actions and activities across the modern enterprise in a way that gives the right system of record to perform these functions. IoBs will ideally be done in an extensible, open way with standards and query language for interoperability and to be for the 2020s what IOCs were for the 2000s.

***TAG Cyber: What are some of the problems SecOps teams encounter when trying to identify, triage, and mitigate incidents using a non-XDR approach? What are some of the impacts?***

**CYBEREASON:** In any domain where workers have to focus on the tool instead of the task, performance crashes. The more the tool becomes transparent, the better the learning curve, the quality of the work, the efficiency, the job satisfaction, the improvement loop, and more. One of the biggest problems is that it takes time and energy to know how to ask questions, to pull together the data, and to do the real job of actually stopping attackers earlier, more completely, and more reliably.

When cars were new, there were laws across the United States about having to have people walk in front of the car with red flags to warn people a car was coming; it's hard to drive fast and safely and to use a car for anything more than a scenic tour in a world like that. To some degree, this is where many SOCs are with their toolkit. The promise of XDR is to remove noise and to bring more context for the whole story of an attack to be understood. The goal is to spend as much time as possible working on the tasks of finding, sorting, and fixing advanced attacks and their damage while improving the craft with as little waste as possible.

***TAG Cyber: How much of incident response can be automated and how much human analysis and action is needed?***

**CYBEREASON:** We deal with an adaptive, intelligent human opponent in ways that are different from IT and other parts of the business. In this world, we have to set the greatest minds in opposition to the adversary. With that in mind, from automation and machine learning to artificial intelligence and beyond, all should be set in service and in partnership to the humans behind the screens.

To that end, much can be automated, however, automation can be used against the defenders if not done carefully. Predictability



means that the opponent can seek to abuse the automation to hide or, worse, to their own ends. Trust-but-verify applies to automation more than anywhere, but it remains a vital ingredient to improving cyber effectiveness and the efficiency of the carbon-based units too.

***TAG Cyber: Cybereason has a focus on ransomware — for obvious reasons: it's a prime attack tactic. What are some of the more concerning ransomware trends your team has seen recently?***

**CYBEREASON:** In addition to the liquidity that cryptocurrency provides, two things are most concerning. First, ransomware is a business model. Calling them “ransomware gangs” is minimizing the threat; it gives the impression of unsophisticated, juvenile organizations. Instead, they should be called “ransomware cartels.” They grow because they are highly profitable, and their business models are growing to rival the extent and sophistication of the largest and most developed legitimate industries in the world. They have supply chains and an insidious set of “as a service” offerings, such as DDoS-as-a-Service and Ransomware-as-a-Service. This trend isn't slowing either; it's accelerating.

Second, these are really RansomOps. Most see ransomware as an evolution of malware. That's somewhat true, however, we need to break ransomware into two components to understand this label: payload and delivery mechanism. Payloads are becoming more devastating and damaging, but that alone doesn't account for their success. It's the delivery mechanism that is most successful. How the ransomware arrives at the target is using the advanced toolkit of the formerly-called APTs, nation-states and top tier attackers. It's the marriage of the two that is so devastating: automated beachheads and initial exploitation, classic compromises of identities and systems, and then the application of hacking skills to explore, expand, exploit. All of this leads to a time-on-target, simultaneous delivery of the payload. And that's the secret sauce for the adversaries to scale and achieve the devastating results and shocking growth of the last three years.

This can be dealt with, but it requires preparation in peacetime, top notch prevention, world-class detection and response, and mitigation of the post detonation damage to limit the blast radius when it gets through.



AN INTERVIEW WITH SEAN LEACH,  
CHIEF PRODUCT ARCHITECT, FASTLY

# INNOVATION TO SPUR DELIVERY OF UNIFIED APPLICATION PROTECTION

Content delivery networks (CDNs) are a backbone of the internet, allowing companies to digitally conduct business in a highly performant and available manner. Once seen simply as delivery mechanisms, CDNs have evolved to protect against cyber attacks. Preventing denial of service attacks was the first cyber challenge posed to CDNs, but over time, customers have demanded more. As cyber criminals took advantage of digital transformation, including the rapid adoption of cloud and the growth in the number and importance of web applications, CDNs have had to keep pace, either by building in native capabilities or partnering with or acquiring companies to fill the security need.

In October 2020, Fastly, a well-known CDN, completed its acquisition of Signal Sciences, an industry-leading WAF and API protection provider. Combining these best-of-breed capabilities under the Fastly brand has opened up new security opportunities for enterprises. Sean Leach, Chief Product Architect at Fastly, shares what the company has been up to and his vision of the future of content delivery.


**TAG Cyber:** *Let's start with the acquisition. Why was the marriage of Fastly and Signal Sciences such a good fit?*

**FASTLY:** We found excellent technology and talented people at Signal Sciences. As two highly like-minded companies, we both maintain a strong focus on empowering developers to innovate while delivering unified application and API protection that includes bot management, account takeover protection, API protection, rate limiting, DDoS mitigation, TLS, and web application firewall (WAF). Signal Sciences greatly enhances our security portfolio, and by thoughtfully leveraging our respective strengths, we are providing customers with performant security that modern app developers, ops, and security teams love.

**TAG Cyber:** *How has DevOps shaped what Fastly is doing today?*

**FASTLY:** Fastly uses modern application development processes that are agile, and we also use continuous integration and deployment (CI/CD) methods, which means we update the Fastly cache fleet almost daily. This allows us to release new code, features, and updates more frequently. And for our customers, the Fastly CDN is built API-first, so developers can make use of all the CDN's features within their own technology stacks. The APIs can integrate directly into a company's continuous integration/continuous development (CI/CD) workflows and work better in an agile, DevOps world. With modern CDNs, developers no longer have to wait for a vendor to make config changes; instead, they can be done as part of developers' natural workflows using their existing tools.

Security engineers can't manage security rules and visibility from many different systems in many different locations: they need a single interface to manage their security policy.



In addition, with our real time configuration and visibility, developers can feel confident that we can get into their rapid deployment flow. Changes will propagate in real time throughout the world, and just as important, visibility is available to make sure no bugs were introduced with their code deployment. If there were, they can quickly be reversed.

***TAG Cyber: The concept of edge computing has exploded in recent years. Why do you think that is?***

**FASTLY:** The explosion of edge computing stems from the convergence of two trends in web applications: increasingly global audiences and rising user expectations for performance and personalization. Outside of major population centers in Europe and North America, central clouds don't have the network reach to consistently deliver a good experience to users, particularly when each individual user expects a personalized response. Edge computing allows developers to combine the power and ease-of-use of cloud computing with the responsiveness and user-centricity of local apps. As more and more users around the world experience edge-based applications, their expectations continue to rise, leaving applications based on legacy architectures further and further behind. Savvy enterprises see edge computing as the next evolution of the cloud. Industry leaders looking for ways to deliver truly delightful application experiences for their end users are turning to edge computing for answers.

***TAG Cyber: What new challenges to content delivery are enterprises facing in our new remote/remote-to-hybrid working world?***

**FASTLY:** Clients and applications are no longer connected from central locations like a corporate headquarters. Users are remote, mobile usage is exploding, and applications are being moved out to the cloud in various regions around the world. Content and application logic need to be as close as possible to both the clients and applications in this scenario. In addition, with the greatly increased threat environment, content delivery networks need to provide more than just performance; security has to be baked in to take advantage of the scale and visibility that an edge cloud provides.

The CDN also has to enable and enhance digital transformation, not get in the way. Only the new, modern CDNs can help with this. Enterprises were forced to stuff five years of digital transformation into five months. All of their tools need to enable this — especially their edge presence.



***TAG Cyber: What trends are you seeing against companies' web-based assets that enterprises must be aware of?***

**FASTLY:** We are seeing several key security trends against companies' web-based assets. First of all, applications, APIs and microservices have grown exponentially in the past decade. This was further accelerated with the COVID-19 pandemic and work-from-home policies driving record traffic to web applications and APIs for business and customer processes. As a result, digital transformation is increasing in velocity and so is the risk at the web and API layer.

Applications have also been split into multiple smaller components (microservices), with the explosion of mobile APIs now providing some of the most critical functionality of the system, and developers are now deploying hundreds of times a day across multiple cloud providers. This means performance and security for east/west traffic (i.e., traffic between two application components) is just as important as north/south traffic (traffic between users and the application).

Lastly, the rate of new technology entering the enterprise has risen exponentially. The rise of APIs, containers, and serverless, and the increase in technology platforms across the enterprise means that in order to get strategic coverage over web applications and APIs, businesses need a protection solution that can deploy anywhere that applications and APIs live. Security needs to be everywhere. That means security must run at the edge, in the cloud, in the data center, everywhere, with a single, easy to use control plane. Security engineers can't manage security rules and visibility from many different systems in many different locations: they need a single interface to manage their security policy.



BRIAN HAZZARD,  
CO-FOUNDER AND CEO, RANDORI

# PROACTIVE ATTACK SURFACE MANAGEMENT FOR RISK REDUCTION

“Attack surface management” is a term that covers a lot of ground, and one which means different things to different security practitioners. The reality is that modern companies’ cyber attack surfaces are already large and ever-expanding. And the speed at which businesses operate, the interconnectivity of systems, the amount of data and applications produced daily, staff shortages, adversary sophistication, and more create an uphill battle for finding and fixing vulnerabilities before an attacker does.

Automation has become necessary for managing the attack surface. Importantly, though, automation can’t just produce a simple identification and dump of, “here’s every exposure you have!” There would be too many “priorities” for security teams to triage.

The team at Randori incorporates their experience as pen testers and red teamers into their attack surface management (ASM) platform, but uses automation and machine learning to ensure efficacy. We spoke with Brian Hazzard, Co-Founder and CEO at Randori, about ASM and how companies can use automation to quickly identify exposures and attack paths.

***TAG Cyber: First, can you provide your angle on attack surface management and what it means for enterprise security teams?***

**RANDORI:** Attack surface management is an emerging category that aims to prioritize organizational risk from an external perspective. An organization’s attack surface is made up of all hardware, software, SaaS, and cloud assets that are accessible from the internet, that process or store your data, and are discoverable. In short, your attack surface includes any external asset that an adversary could discover, attack, and use to gain a foothold into your environment.

Enterprise organizations use attack surface management to gain a better understanding of their perimeter and to help prioritize work and vulnerabilities in their noisy vulnerability assessment solutions.

***TAG Cyber: Ransomware has been a big(ger) problem lately. How can companies really defend against this, other than disabling links and downloads in email – which seem to be the best and easiest ways attackers get into systems?***

**RANDORI:** Ransomware attacks are painful for organizations and garner much attention in the media. Yet they are simply the latest symptom in a deeper problem – the inability to assess and proactively reduce cyber risk. Facing a growing onslaught of attacks, security teams are looking to adopt more proactive ways to reduce their operational risk from ransomware. With 40% of attack techniques that end in ransomware beginning with a pivot through the attack surface, ASM is the first step in preventing ransomware.



Three things companies should focus on:

1. **Know What's Exposed:** By the time an attacker is on your devices and thinking of holding you for ransom, it's already too late. The real battle is won in preparing contingency plans when your security perimeter fails.
2. **Harden Your Top Targets First:** Know where attackers are most likely to strike first. Organizations often have tens of thousands of exposed assets on the internet; the key is to find the ones hackers will target first. This will provide you with an external perspective of your business using the same advanced techniques threat actors use to identify your most tempting ransomware targets – helping you zero in on your greatest risks quickly.
3. **Test Your MDR & IR Capabilities:** Your attack surface is always changing and ultimately, a hacker will gain access. When this happens, you need to know if your security program can contain the threat. Using continuous automated red team platforms can help you build a scorecard of your MDR and IR effectiveness that can be used to build the case for further investment or assess the effectiveness of previous investments and create valuable opportunities for your team to gain experience before a real incident occurs.

***TAG Cyber: What are some of the key findings from Randori's recent "The Rising Cost of Ransomware" survey?***


**RANDORI:** We discovered that ransomware struck nearly half of businesses within the past 24 months and forced CISOs to agree that the threat should be considered a "cost of business." After suffering a ransomware attack, 87% of decision makers changed their security strategy, with 40% increasing their spend. Companies shifted their strategy to increase focus on:

- Prevention (51%)
- Resiliency (48%)
- Visibility (47%)
- EDR & Disaster Recovery (46%)

With shadow IT and web-based exploitation accounting for a growing share of ransomware attacks and one third of all breaches, hardening and reducing an organization's attack surface has become a must. Our research shows that security leaders rank ASM as one of the three things to do to reduce the risk for ransomware.



With Only 5.5% of all vulnerabilities ever exploited in the wild, being able to prioritize the ones hackers are most likely to target is essential.



***TAG Cyber: How does your platform address the different components of a cyber attack?***

Randori: Randori helps organizations understand true risk with our ASM and Continuous Automated Red Teaming solution. We do this by:

- Finding Unknowns: Corporate environments are dynamic and diverse environments making blind spots and shadow IT a constant challenge. Randori automatically discovers your true attack surface, finding unknown assets others miss. This is an essential capability for any security team at organizations with large environments and heavy digital asset footprints.
- Vulnerability Prioritization: Randori provides vulnerability management teams critical insight into the attackability of external-facing assets. With Only 5.5% of all vulnerabilities ever exploited in the wild, being able to prioritize the ones hackers are most likely to target is essential. Randori's patented Target Temptation engine and industry-leading prioritization features make prioritizing vulnerabilities and reporting progress easy.
- Focus on Operationalization: While other ASM vendors focus on mean time to identification (MTTI), Randori understands that identification is just the beginning and the real value comes from action. Our platform has been designed to reduce mean time to action and accelerate your team's ability to respond. Our bi-directional APIs and ecosystem of integration partners make it easy to integrate Randori with other asset and vulnerability management solutions and are being used by our customer to provide critical context on their external attack surface.

The Randori Platform was built to think and act like today's nation-state and ransomware actors. Our attack platform automatically identifies the internet-facing assets hackers will attack first, exposing where and how attackers will strike your environment.

***TAG Cyber: With so many vulnerabilities. How can companies effectively manage all the output they receive from your platform?***

**RANDORI:** ASM and vulnerability management are always going to have their places in the security world, and they will always overlap. Different components work together to address the overall goal of reducing overall exposure. There are many different ways to break into a house, and nothing designed to be accessible will ever be entirely secure. The key is to use the resources at your disposal to make attacking you as tricky as

possible. Chances are, if you've had a vulnerability management platform over the past several years, you've watched its value decline. As it spits out longer and longer reports with no prioritization, you've had to rely on waiting to be attacked to see where you are most vulnerable. But if you're waiting to react to an attack, you've already lost.

ASM is about proactively seeing yourself through the attacker's eyes so you can close their points of entry before they find them. You can use the attackability metrics you receive from ASM to reduce your attack surface and execute restrictions until you have no doors big enough for an attacker to squeeze through.







**ANALYST  
REPORTS**





# USING SELF-HEALING TO ACHIEVE DEVSECOPS

ADAM LEWINTER

---

## INTRODUCTION

Modern security teams have ever evolving responsibilities. They continue to be responsible for ensuring the security of the enterprise environment, but the rapidly changing landscape of applications and their importance to the success of a company has added more responsibilities and complexity. Delivering applications has always been a cross-team effort, and now security has become integral to ensuring success. However, as security teams have become more integrated, the selection process for security tooling has become significantly more complicated.

Security teams no longer have the political power to just impose their will on the rest of the company and force people to use security tools. This is a good thing, as the days of security being the team of roadblocks and friction did not ultimately lead to a secure corporate environment. Development and operations teams now have input in selecting security tooling which has led to buy-in and greater adoption of security technologies.

That said, while the goal of security teams has not changed, the criteria for selecting a security tool has. Security tools are now expected to protect applications in a wide range of environments while also maintaining the velocity. As more and more production environments move to, or are born in, the cloud, cloud security posture management (CSPM) has become an increasingly important part of security programs.

Traditional cloud security posture management tools utilize automation to identify and remediate issues in runtime which allows them to provide protections against attacks without slowing down development. However, addressing issues in runtime is too late in the process and can lead to maintenance issues, such as configuration drift, or persistence of unidentified issues. This creates back pressure on development and deployment teams, which ultimately slows down the ability for engineering teams to release new features in a timely manner. Therefore, a new approach is needed that identifies and remediates issues before deployment, and Infrastructure as Code (IaC) provides the mechanism to do it.

## INFRASTRUCTURE AS CODE BENEFITS

Security tools have traditionally been very limited in their view and context, and they typically lack the understanding of the controls available in an environment to remediate issues. For example, if a vulnerability is discovered in code, but the tool doesn't know if there is a web application firewall (WAF) that can block a payload trying to exploit the vulnerability, then the tool cannot know whether the vulnerability is exploitable. This lack of context makes it impossible to determine if other tools and controls in the environment are able to handle the issue thereby making it impossible to determine the true risk of the environment.

With infrastructure as code all the resources and connections between those resources are defined in code. This means scanning can easily determine what controls are available and what they will be able to address. It also means that if a vulnerability is found, the impact on the broader environment can be quantified. If a Static Application Security Testing (SAST) or Software Composition Analysis (SCA) scanner finds a vulnerability in the application code, and a WAF sees a malicious inbound payload, the IaC can determine if a path to the vulnerability exists from the internet.

The holistic view of the entire infrastructure provided by IaC enables a new generation of tools to accurately assess risk and prioritize remediation. It also allows security teams to determine where a remediation action is best taken. Some SQL injections are very complicated to fix in code because they have a large impact on other parts of the application. IaC provides the information required to visualize the breach path and then analyze it to know where the optimal place to break the path is located. This provides teams better visibility into risk when deciding whether specific issues need to be fixed immediately or can be fixed in the future. A team can choose to fix the issue where it requires the least effort, thus breaking the breach path and eliminating the risk with the least disruption. This provides teams with more time to decide how to address the more complicated underlying issues.

## SHIFT LEFT

Traditionally, most CSPM tools focus on keeping the runtime secure by utilizing automatic runbooks. They scan a runtime environment after deployment for issues and remediate them based on predefined processes without having to involve any human element. While this might seem like a good solution at first, there is a usability problem from a development and operations perspective. Automatically changing the runtime configurations means operations teams don't understand what the runtime configuration is.

When automatic changes happen at runtime, the configuration files that are stored in code repositories or other locations are not necessarily accurate to the current state. This configuration drift means undocumented changes can run in production. In addition, if there are any issues in the runtime environment, there is no guarantee there will be an alert generated as the automatic runbooks might solve the issue before they are discovered by other tools. This means that unknown issues can persist in environments, and when a new release is pushed it can clobber an automated change or expose an issue for a period before the automation fixes it again—leading to an insecure environment. These inherent flaws of applying security controls in runtime are not ideal and become very troublesome for ephemeral cloud environments. A new approach is needed, and the solution is to shift left by enforcing the same controls during the development phase.

## BENEFITS OF SHIFTING LEFT

This is no easy task as security tools must not slow down the development process, and introducing new controls often leads to developer frustration. However, with the increased adoption of infrastructure as code the ability to enforce security controls sooner without interrupting or frustrating developers is possible. Scanning the infrastructure as code and reporting issues in development allows developers to interact with the security data in their normal process to fix issues before they get to production. Another major benefit is the state of production has a higher likelihood of matching what development teams think it is, which reduces the fragility of deployments and removes the possibility of clobbering an automated fix with the next deployment.

Traditional CSPM tools that provide protection in runtime allow security teams to be compliant with corporate policies and regulations. While this is the goal of any security team, they may not always be familiar with the cost created by fixing the issues in runtime. As discussed, there is back pressure on development and operations teams due to the configuration drift and potential for unknown issues. That makes these issues a real hazard for development teams as unrecognized technical debt can have widespread effects and derail a development roadmap. By identifying and fixing the issues before deployment, issues become visible and there is a clear trail of what has changed so that there is no configuration drift. This means that by providing the visibility sooner the tool helps drive efficiency in addition to security.

Changing the way developers interact with security data by bringing it into their normal development process is also a challenge. This makes the implementation details critical to the success of shifting left and enforcing security controls during development rather than runtime. Automation is key to reducing the manual workload of any process and is one of the reasons CSPM tools have found success. However, a new generation of automation is needed to solve the inherent issues discussed about automated runbooks above. That new generation of automation is self-healing.

## INTRODUCING SELF-HEALING

Imagine a scenario where a cloud developer writes IaC to deploy a database cloud instance within a sensitive production environment using a production cloud account. The developer commits a mistake in the code that leaves the database unencrypted. In this scenario, self-healing technology will detect the mistake in code in the deployment pipeline and intelligently apply and generate remediation code based on runtime awareness of the production environment. The auto-generated code will self-heal the mistake and enable database encryption before deployment and will leave an audit trail that clearly indicates what was changed.

The ability for a software tool to automatically detect issues and remediate them before deployment is at the core of self-healing. Self-healing uses remediation preferences selected by the end-user to determine what steps to take when an issue is detected. Based on the configuration, self-healing can be classified as supervised and unsupervised. With unsupervised self-healing, the remediation is done automatically based on a runbook, a defined set of rules, or other criteria that is defined prior to any action being taken. Traditional CSPM tools that detect and automatically remediate issues in runtime would be classified as unsupervised self-healing applied in runtime.

Supervised self-healing is when an issue is automatically detected and a remediation action is suggested, but not automatically implemented. This gives a human operator a chance to review the suggested change and make the final decision as to whether to implement it. Most alert-based tools across other cyber security areas follow this design, although those that identify problems without recommending a specific fix would not be considered self-healing.

## UNSUPERVISED OR SUPERVISED SELF-HEALING

Each version of self-healing has benefits and drawbacks. The main benefit of supervised self-healing is that the oversight into the process typically makes teams more comfortable with implementing the solution. This is even more important when discussing self-healing in a development process where remediation actions make code changes. Providing suggested changes to developers through their normal development tools matches already known processes for other parts of development and would be easier for them to adopt.



However, tools that only identify issues and leave the task of figuring out how to remediate and prioritize changes to an individual just adds to the noise teams deal with daily and decreases their efficiency. Relying on tools to find issues—and then people to go fix them—is one of the main issues causing DevSecOps to be so elusive. Another drawback is that there is no guarantee the security change will be implemented, and this leads to security and development teams being at odds with each other.

Unsupervised self-healing removes the friction and manual intervention requirement by automatically committing fixes when issues are found. It does not increase the workload of developers and fits seamlessly into the development process which makes it easier for security teams to implement within an environment. Unsupervised self-healing is also an ideal solution for IaC as it provides an automatic way to enforce security and quality standards on complex infrastructure architectures.

However, automatic changes to a codebase are uncomfortable for development teams. The code is the domain of the developer and automatic changes force them to give up complete control over it. The automatic changes to address security issues might meet the needs of the security team, but without developer buy-in, the solution will never be implemented.

## CONCLUSION

Self-healing provides a lot of benefits for developers, operations, and security teams, but discomfort with the level of automation required is a major challenge. Developers have just started to accept the automated runbooks of traditional CSPM tools and immediately pushing more automation is bound to be met with resistance.

However, the level of automation associated with self-healing doesn't need to make people nervous. A successful strategy to shift left incorporates both supervised and unsupervised self-healing approaches. Supervised self-healing provides oversight and control to the code base for development teams that will help with initial adoption. Automation can be used to identify issues and suggest changes to remediate them in the tools developers already use. Then, once developers have become comfortable with the quality of the suggested changes, more automation around implementing the changes can be adopted.

The implementation strategies will differ for each team and perhaps even between applications, but any environment using IaC should consider introducing self-healing. The benefits provided by self-healing allow organizations to shift left into a more DevSecOps practice with confidence.

# AUTOMATION AS THE KILL SWITCH TO MALICIOUS BOT ATTACKS

KATIE TEITLER

---

Bots are a necessary part of the internet. They allow search engines to index sites, they allow businesses to offer automated customer chat functionality, they help businesses identify website performance issues, they help retailers and social networks recommend relevant content for users, and more. But there is a nefarious downside to bots: cyber attacks. Cyber criminals are increasingly using automated malicious bots to exfiltrate data from companies' websites, execute denial of service (DoS) attacks, take over account information, and more.

This report explores how focusing on automation to determine good from bad bots is the key to threat mitigation.

## INTRODUCTION

An estimated 30% to 40% of internet traffic is bot traffic. Bots are, simply, automated scripts which offer a number of benefits. They allow search engines to index sites, they allow businesses to offer automated customer chat functionality, they help businesses identify website performance issues, they help retailers and social networks recommend relevant content for users, and more. In cyber security circles, we hear the word "bot" and automatically (pun intended) assume nefariousness.

That said, the inherent functionality of bots makes them a perfect “dual use” tool, that is to say, one that can be used both for good and for harm. It’s not complicated for someone with basic coding capability to write a script for an automated bot, and therefore someone could write something that helps users, or they could write something that harms them. The existence of a bot, as identified by automation, is not a decisive indicator of goodness or badness. But because of the commonalities between human actions and bot activity (bad bots are specifically designed to mimic human actions), identifying bad bots can be difficult. This is where many bot mitigation technologies fall down in their pursuit of stopping the bad bots that can steal login credentials, gain unauthorized access to accounts, and spread disinformation across the web at frighteningly fast speed.

What’s more, bot operators have grown savvy as the market has evolved; they use tricks of the trade to make their bots blend in with normal traffic. Bot operators, like defenders, look at historical data to determine what “normal” human activity might look like. They use that knowledge to mimic humans, and use residential proxy services and anti-detect browsers to disguise their presence, which makes identifying human traffic from non-human traffic difficult. Behavioral analysis, therefore, is not always a foolproof way to identify bots, especially not malicious bots. And rules-based detection, which was common with first-generation bot mitigation tools, is too easy for bad actors to manipulate to be effective.

Later in this paper, we’ll explore how to detect and prevent malicious automation. But now we’ll provide a sneak preview of why automation, not just the use of automation, but specific characteristics of automation, are a key to bad bot prevention. In short, old methods of detection that rely on IP addresses, bad user agents, and behavioral analysis aren’t enough to keep up. Today, it’s all about the ability to detect the immutable presence of automation, client side, when- and wherever bots interact with websites, applications, and APIs.

## WHAT’S AT STAKE?

Malicious bot operators focus their attention in three main areas:

- Web
- Mobile apps
- APIs

Why these interfaces? Quite simply, because web and mobile apps are the edge interfaces through which users interact and transact with businesses. They are feature-rich in order to make users’ experiences simple, allowing them to click links, fill in forms, buy goods and services, and more. These features lend themselves to targeting by cyber criminals, via bot activity or otherwise, because so much proprietary and useful data can be stolen from these interfaces. Plus, as mentioned earlier, websites and mobile apps are natively designed to interact with bots — the legitimate kind — and third-party functionality to work properly. Bot activity is thus expected, making it harder to identify bad bots.

With mobile apps, in particular, security posture relies (in part) on the version in use. While a developer may roll out the latest security features and functionality diligently, it is up to consumers to update to the newest version — which cyber criminals know may or may not happen. Software vulnerabilities are rampant, and bad actors are relying on those vulnerabilities to execute their attacks.

APIs are the primary way applications and websites talk to each other; APIs are built for machine-to-machine communication. Tens of thousands of public APIs are available from websites and applications, and APIs connecting various IT systems skyrocket that number into the uncountable realm. Further, the threshold for API communication is low, in service of allowing fast transactions, which



makes them susceptible to malfeasance (and why API protection is becoming a category unto itself). And since APIs are a connection point that are, by design, meant to be open and accessible, they are inherently weaker than other parts of the technology stack. This makes them juicy targets of attack, including bot attacks.

Web, mobile app, and API owners might be tempted to just block bots. But for the reasons stated previously, this cannot be done. Not only will doing so prevent the positive aspects of bots on functionality and user experience, but blocking all bots may cause bad bot operators to mutate their scripts, in essence, causing defenders to chase a moving target.

## THE IMPACTS OF BAD BOTS

Malicious bot attacks affect various repercussions but the main motivation behind them is digital fraud and abuse – a giant category that encompasses many things. Notably, while this report is written for cyber security and IT operations professionals given the fact that these groups generally govern bot mitigation solutions, malicious bot attacks affect a bigger swatch than tech teams; sales, marketing, finance, customer service, and production/operations are and can be affected due to a bot attack. Below are the top three concerns about tangible impacts on organizations, as per TAG Cyber's enterprise clients, when a bot attack occurs (in no particular order):

- **Data breach:** A bot attack can result in unauthorized access to systems, data, and accounts. From PII to intellectual property, nothing is out of scope when bot operators gain access by stealing credentials and user information to infiltrate your organization.
- **Fraud:** Not surprising given the heading of this section, fraud is a main goal of malicious bot attacks. Some of the desired effects include: Account takeover, fraudulent account creation, carding and cracking (draining rewards and financial accounts of stored values), stolen credentials (which can be sold on the black market), impersonation and identity theft, making purchases online illegally (often using stolen credentials and/or payment information), executing ransomware.
- **Reputational damage:** Businesses can experience a loss of customers, loss of revenue, customer experience degradation, the spread of disinformation related to their company or company executives, increased spam, and more when they are the victim of a bot attack.
- **Loss of marketing dollars and advertising revenue:** Bad bot operators may divert goods or money away from a business, provide phony "leads" to companies that rely on form fills for prospecting and customer service, plump websites and mobile apps with inflated traffic statistics/analytics which give companies a false sense of reality and/or increase advertising spend, and more.

The methods malicious bot operators use to execute attacks can also vary. The main techniques seen in the wild include:

- **Credential stuffing:** Credential stuffing involves leveraging automation to conduct mass log-in attempts that are used to verify the validity of stolen username/password pairs and then abuse them. It is one of the most popular techniques to take over accounts. Credential abuse can also lead to other types of financial fraud, increased customer complaints, and more.

- Application denial of service: Denial of service (DoS) might seem like a thing of the past due to the sophistication of content delivery networks. But bot operators have become more sophisticated, targeting the application, instead of the network, to:
  - Flood the bandwidth of web and mobile properties, rendering them unavailable or frustrating to users.
  - Prevent companies from fulfilling orders (e.g., retail, eCommerce) or scheduling appointments (e.g., healthcare, financial services).
  - Hoard inventory, without any intention of a purchase, to prevent companies from receiving orders.
  - Purchase large quantities of in-demand items (when bulk discounts are available), and then sell that inventory for a significant markup to make a profit.
- Content scraping: From the wording on your website to competitive intelligence, a bot attack can devalue your brand through:
  - Web and price scraping: imitating the language or pricing on your website or mobile app to lower your competitive advantage and uniqueness in the marketplace.
  - API scraping: extracting data behind the API that is not public visible on web or mobile app properties.
- System takeover: As is likely obvious from the name, system takeover can occur when a malicious bot scans for system/software vulnerabilities and exploits them. This often leads to unauthorized access, data theft, and other acts of fraud.

## DETECTING AND PREVENTING MALICIOUS AUTOMATION

Identifying and stopping bad bots has no silver bullet, but a set of actions that work together to form a kill switch when malicious automation is found. Many commercial bot mitigation tools exist on the market today, and each has its own approach to detection. Regardless, at a fundamental level, every bot mitigation platform should be able to protect mobile, web, and APIs distributed across the organization, and continuously ingest data to analyze and profile requests (to determine if the requests are real or bot-driven).

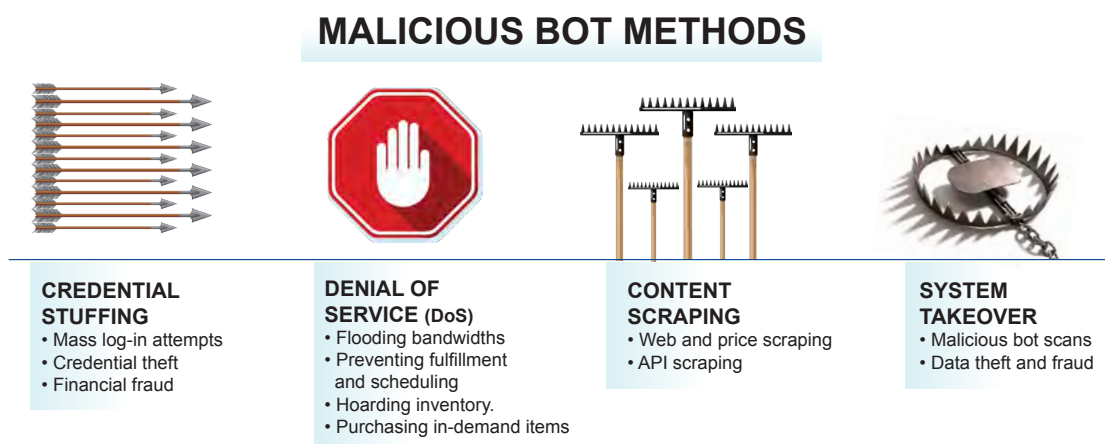


Figure 1: Malicious Bot Methods

Beyond the basics, next-gen bot mitigation solutions are moving detection to the edge, that is, to the client application — the browser, mobile app, or API endpoint — using sensors. Traffic inspection will reveal the immutable evidence of automation when a bot interacts with a client by looking at attributes and signals. Examples of the information collected include headless browsers, automation frameworks, and mobile emulators.

One important caveat to the comment about frameworks is their dual-use nature. Thus, the mere presence of these tools and processes does not necessarily indicate nefariousness. Common DevOps tools can be repurposed for malicious intent. For instance, open source browser testing frameworks like Puppeteer, Playwright, and Selenium can be used to conduct automated attacks, but they're also used by developers to build and test software. That said, client-side inspection will reveal if these tools are being used to make requests, and then inferencing will help determine if the request is good or bad.

When the request is deemed malicious through the interrogation process, it is denied. The whole process could stop there, but in some newer solutions, we've seen the deployment of deceptive techniques, similar to a decoy or honeypot, that flood malicious automated requests with real-looking and acting signals such as fake responses and alternative origin redirection that will deter the bot and frustrate attackers.

Another newer deterrent technique is for the bot mitigation platform to automatically send a cryptographic challenge as a proof of work when a bot is identified. This increasingly difficult challenge, requires the requesting machine to respond and ties up resources without sending up red flags — making automated attacks computationally expensive to conduct.

A modern commercial solution also requires data analytics, to analyze historical data about attacker techniques and patterns which can be used to continuously improve detection over time. Further, threat intelligence about adversarial techniques and traffic patterns should be incorporated into a solution, either natively from the provider's internal research team or via third-party integration with industry-leading threat intelligence feeds.

Needless to say, more traditional techniques, such as MFA, zero trust access controls, traffic monitoring, HTTP request and response data analysis, behavioral profiling, and blocking anonymous proxy servers also contribute to the kill switch that prevents malicious automation.

While various techniques and processes are used in malicious bot prevention, it's that first important step — revealing the immutable evidence of automation — that may hold the key to preventing bot attacks. Though automation is not the only — nor is it necessarily an — evidence of maliciousness, all

<b>Traditional bot detection</b>	<b>Next-gen bot detection</b>
Accepts client requests then looks for suspicious behavior	Detects automation in real-time, without accepting client requests
Misses bots from legitimate IP & user agents	Applies zero trust methodology
Requires continuous learning and rules management	No rules to manage or heuristics to learn
Requires a high level of expertise to maintain	Minimal maintenance, keeps defenses invisible and responds with low feedback
Becomes ineffective when adversaries retool	Identifies evidence when automation is present to immediately adapt to retooling
Is easy to reverse engineer	Cannot be easily reverse engineered

**Figure 1: Malicious Bot Methods**



bot attacks have one thing in common: automation. If your organization can firstly identify the use of automation then deploy step-up techniques to confuse and frustrate attackers, the probability of an automated malicious attack decreases significantly.

## EVALUATING COMMERCIAL BOT PROTECTION PLATFORMS

A commercial malicious bot prevention solution will allow businesses to identify when their web, mobile, and API properties are being targeted or attacked by automated bots with harmful intent and distinguish them from “good” bots.

With fewer bot attacks against their properties, 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.

When evaluating malicious bot 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 automated malicious bots?*
  - a. How are you monitoring external sources for fraud against your company and customers?
  - b. Do you prioritize web- and customer-facing properties as risk factors?
  - c. What/where is the greatest risk?
    - Web?
    - Mobile?
    - AP/s?
  - d. *What is the business impact if attackers exploit those systems and*
    - Disable your web or mobile sites?
    - Prevent your company from collecting data from customers?
    - Prevent your company from selling goods or services online?
    - Steal customer, employee, partner, or system credentials?
    - Mimic your company brand to spread disinformation, sell counterfeit goods, or create smear campaigns against your company?
  - e. *What is the impact of account creation fraud on your business when a stolen identity is used to make purchases?*
- 2) *Tools - Which commercial tools are you aware of that might help reduce this risk to your Internet assets? How might these be identified, researched, and tested?*
  - a. What types of tools are used today to detect these types of problems?
  - b. Who is involved in source selection and use?
  - c. How does the organization improve its research and source selection in this area?
- 3) *Assets - What types of web and mobile properties do you maintain?*
  - a. How many web/mobile properties does your company maintain?
  - b. How are you tracking updates and changes to your web/mobile assets?
  - c. What sensitive or proprietary information do you provide publicly that could be used to harm your business?
  - d. How are you monitoring for violations against your brand or copyright issues?

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

- 1) *What techniques are used to detect malicious bots?*
  - a. Identifiers (e.g., IP addresses, geos, headers)
  - b. Signatures
  - c. Behaviors
  - d. Evidence of automation
  
- 2) *What analytics are provided to analyze bots and their actions?*
  - a. What data sources are ingested?
  - b. How is/can data be broken down by attack vector, mobile, web, API?
  - c. How easy/difficult is it to compare human-driven activity with bot activity, and further, good bot activity vs. malicious bot activity?
  
- 3) *What categorization does the platform allow for?*
  
- 4) *How are policies created?*
  - a. Who is in charge of policy building and maintenance, the customer or the provider?
  - b. Does the platform include pre-configured policies?
  - c. Can custom policies be built?
  - d. Are playbooks included?
  - e. How easy/hard is it to update or change policies?
  
- 5) *What actions/remediation are taken when a bad bot is identified?*
  - a. Block
  - b. Monitor
  - c. Sandbox
  - d. Request additional identification
  - e. Serve decoy content
  - f. Redirect traffic
  - g. Control access/rate limiting
  - h. Identify the origin/attempt takedown
  - i. Proof-of-work challenge
  
- 6) *Does the provider employ a research team to hunt new threat tactics, techniques and procedures?*
  - a. What new or novel research have they published in the last 6-12 months?
  
- 7) *How is the platform deployed?*
  - a. What architectural changes might be needed to deploy?  
Are any special system permissions required?
  - b. How long does deployment take?
  - c. What system/access rights does the platform require?
  - d. What type of performance impact is expected?
  - e. How much ongoing maintenance is required?

- 8) *How much care has been taken to protect the platform's detection methods?*
- a. Can the detection methods be easily reverse engineered?
  - b. What methods are taken to obfuscate client-side scripts?

## CONCLUSION

Malicious automation from bots poses a major threat to businesses. Stopping malicious bots is becoming harder and harder, given attackers' efficacy in building bots that look and act like legitimate traffic and/or human traffic. Early-generation malicious bot detection that uses fingerprinting, rate limiting, and rules- and behavioral-based techniques are not sufficient to stop advanced bot operators. Using automation at scale—the same way cyber adversaries do—to identify automated requests can stop a malicious bot before a request is served, thereby preventing exploitation against companies' web, mobile, and API entities.

Next-generation malicious automation detection incorporates deep inspection and cryptographic challenges, all using automation at scale, to deter bot operators and prevent exploits.

# TOWARD SECURE BUSINESS NETWORKING 2.0

EDWARD AMOROSO

---

Secure business networking 1.0 has been characterized by perimeter-based enclaves communicating across private carrier MPLS, VPN, and B2B connections to support branch office, remote worker, and supplier connectivity needs. Evolution to secure business networking 2.0 involves greater use of cloud services for network control, as well as increased flexibility in WAN management, security protection, and secure access.

Businesses tend to describe their infrastructure in the context of an ecosystem of cooperating groups. These include employees, customers, suppliers, third-parties, consultants, regulators, and other supporting entities. As these groups have continued over the years to spread out across geographies and domains, and as more of the functions supported by such groups have been outsourced, the role of the underlying communication network has grown in importance.

Originally built on private circuit-switched infrastructure, business networks have undergone massive transformation to the distributed arrangement of voice, data, and video networking solutions in place today. Security has also undergone massive change across business networks with the unusual conundrum that despite massive increases in deployed network security controls, overall cyber risk has grown considerably.

The basis for this increased business network risk involves many factors. For example, Internet connectivity expanded the attack surface for business infrastructure exponentially. Similarly, as the enterprise local area network (LAN) expanded in size, scale, and scope, the likelihood of compromised insiders or malware being present also increased considerably. Mitigating risk properly in modern business networks requires solutions to these difficult challenges.

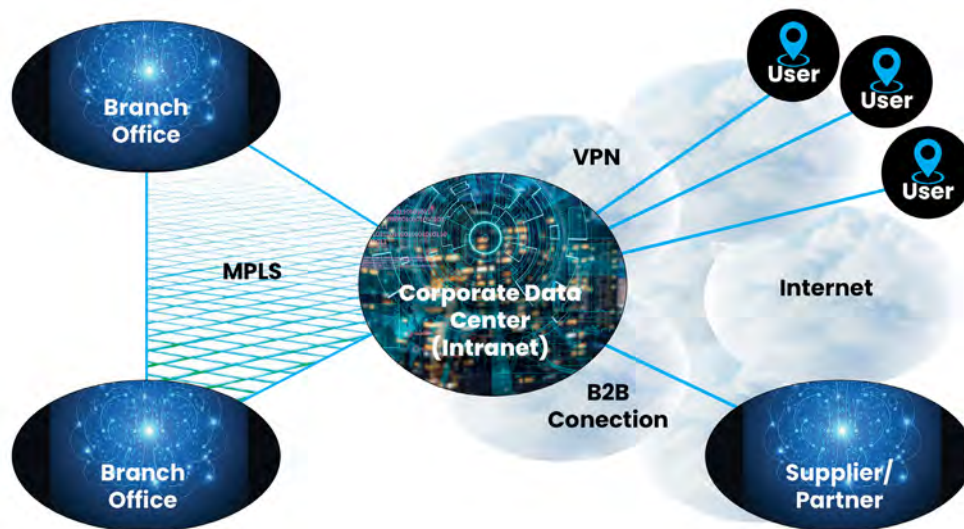


In this article, we address a major transformation that is occurring today – one that is characterized by an oversized influence of cloud-based technology, services, and infrastructure on how business networks are being organized. Specifically, we introduce the idea that present secure business networks (which we call 1.0) are being redefined toward new cloud-based networking methods (which we call 2.0) that match emerging use-cases for effectively.

## SECURE BUSINESS NETWORKING 1.0

Since 2000, business networking has been dominated by three use-cases: (1) Branch offices of an organization have had to be tied together into a secure network, which is organized around a centralized data center; (2) employees and other users have required secure access to the data center over a wireless network or the Internet; and (3) partners and suppliers have required access to the data center via the Internet or across a private connection.

Deployed solutions for these three cases have been largely consistent – and have helped to define the network services industry: (1) Branch offices are connected to corporate data centers using multi-protocol label switching (MPLS) services in a hub-and-spoke manner; (2) remote users access the corporate Intranet through virtual private network (VPN) solutions; and (3) dedicated virtual or even physical business-to-business network connections provide access for third parties to the data center (what we used to call the extranet).



**FIGURE 1.** Secure Business Networking 1.0

These services, which can be viewed collectively as Secure Business Networking 1.0, have made sense for nearly two decades because the security at each enclave – whether data center, branch office, or corporate headquarters – has been supported by two concepts: First, each enclave is bounded by a perimeter, which makes the internally stored data more trusted by default. The idea of insider versus outside thus emerges with respect to an enclave.

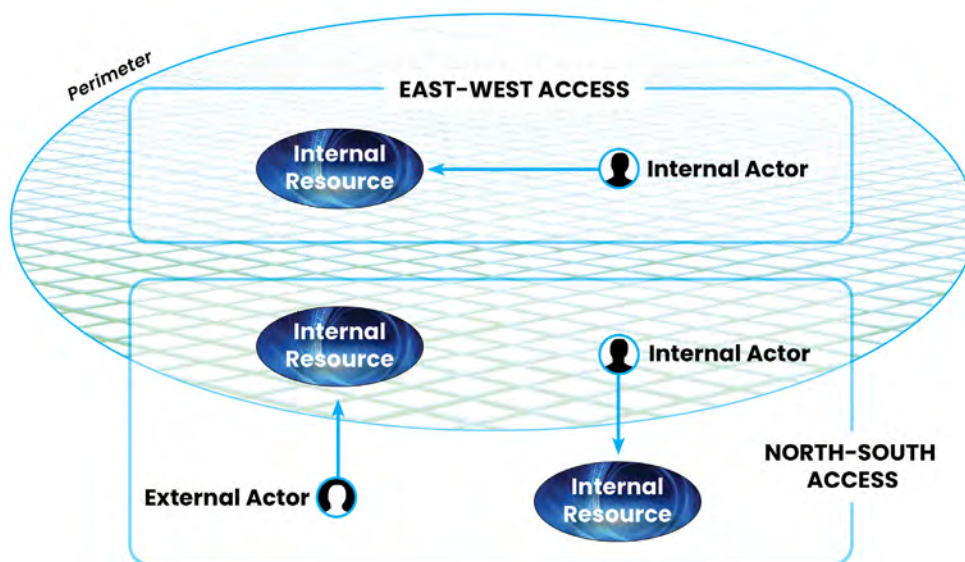
Second, and more importantly, the enterprise has allowed the corporate Intranet to burgeon with applications, systems, services, sub-networks, and other resources that are shared by trusted entities within the perimeter. This approach makes networking much more convenient and allows for easier deployment of new technologies. Users on an internal LAN, for instance, typically do not have to deal with multifactor authentication to access the data center.

With decentralized computing, however, and a clear shift to public cloud use, the network approach embodied by powerful centralized Intranets and hub-and-spoke access to data center-hosted resources no longer makes sense. Some observers have built models to describe how this new arrangement benefits from virtualized, cloud-hosted support – and this does make considerable sense in emerging network design.

## TOWARD SECURE BUSINESS NETWORKING 2.0

One of the main security issues that has emerged with respect to secure business networking 1.0 involves so-called East-West lateral traversal threats<sup>1</sup>. The problem is that when a perimeter is clearly defined and used to differentiate trusted internal users from untrusted external users, the result is that internal network security tends to become quite lax. That is, internal users are allowed to access internal resources based solely on their local area network proximity.

This creates the unfortunate situation where intruders must only puncture a virtual hole, usually with an inbound phishing attack, or a physical hole, usually via a malicious human insider, in order to gain unauthorized access to enterprise data and resources. Once the hole has been made, the malicious actor can take advantage of the East-West vulnerability to laterally traverse and explore the enterprise in search of valuable data (see Figure 2).



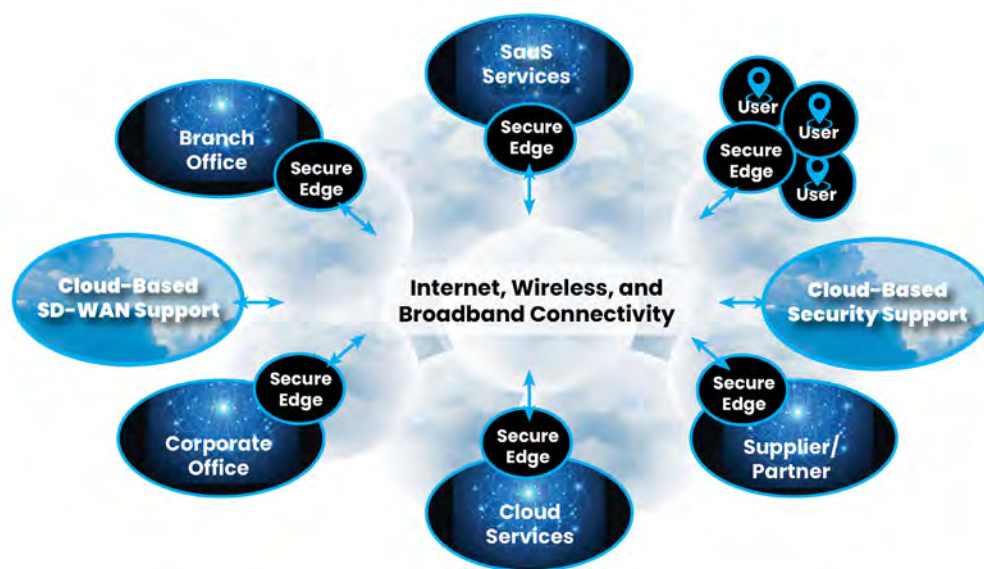
**FIGURE 2.** East-West and North-South Access

To address this East-West vulnerability, enterprise architects have begun the process of de-perimeterization, where workloads, applications, and services are moved from the corporate data center into public clouds. This trend, which began roughly a decade ago, has accelerated to the point where public cloud services from Amazon, Microsoft, and Google have become standard components of virtually every organization’s infrastructure.

The implication of public cloud usage on networking has been significant. Where the corporate data center served previously as the hub of all networked communications, the new cloud and SaaS-based approach is much more distributed. For example, where employees would have needed access to the corporate LAN to perform actions such as checking their paycheck stubs, now they can access these functions over the Internet to the cloud.

In addition, enterprise teams aligning with a public cloud-oriented infrastructure benefit from the increased scalability and flexibility of their applications and services. Businesses can be more responsive to their customers, and third-party access, which has always been a difficult security issue to mitigate, is greatly eased. Users, branch offices, and suppliers all experience similar secure access use-cases.

This new arrangement helps define the on-going shift to Secure Business Networking 2.0. Consisting of a cloud-first approach to network management, support, maintenance, and operation, the new scheme has been the subject of much review and assessment<sup>2</sup>. In practice, the primary implication is a shift from a hub-and-spoke architecture to a new set-up that includes a hybrid configuration of clouds, SaaS services, and legacy systems (see Figure 3).



**FIGURE 3.** Secure Business Networking 2.0

The secure business networking 2.0 model involves the use of secure edge processing to make local decisions about network route selection, including potentially 5G services, via SD-WAN functionality. The approach also references the local computation required to initiate a secure connection over potentially insecure communication. This is in contrast to the label separation involved in traditional MPLS services from telecommunications carriers<sup>3</sup>.

The business implications of this new networking model center on the enablement of cloud and SaaS-based services across the enterprise. Such decentralized architectures are consistent with de-perimeterization initiatives and have created an interim hybrid configuration for most organizations as they begin this transition. It goes without saying that cloud and SaaS economics are also attractive and produce much lower operating costs for IT services.

The vendor implications of this networking shift are uneven, depending on the type of vendor and the legacy positioning. Security vendors, for example, see this new model as a major opportunity to integrate their solutions into the new enterprise. This includes providers of cloud access security brokers (CASBs), data leakage prevention (DLP), secure web gateways (SWGs), next-generation firewalls (NGFWs), and secure access providers.

Tier 1 network service providers, however, will see a massive transition of legacy services such as MPLS toward new sale opportunities. Considerable business growth, for example, will come from investments in the underlying fiber and broadband infrastructure required to provide physical transport of these secure business networking 2.0 services. This includes both backbone and last-mile connectivity.

In addition, the Tier 1 providers have the experience and means to deliver high quality, high availability, and dependable services to their business customers. Security vendors too often forget the challenge of such reliability and resiliency requirements, so the carriers will likely provide the underlying service harness on which most secure business networking 2.0 capabilities are actually delivered to business and government.

## ACTION PLAN FOR ENTERPRISE

Enterprise network, security, and IT teams are advised to create an action plan immediately to guide the next five years of transition toward secure business networking 2.0. We select five years as a horizon, because existing master service agreement (MSA) contracts, compliance initiatives, and regulatory burdens (e.g., Communications Assistance for Law Enforcement (CALEA) support for electronic surveillance) will complicate the transition somewhat.

Many details must be included in the action <sup>4</sup>plan with input from the IT organization, networking team, and CISO-led group. These details span operational issues, customer requirements, and security objectives. A high-level checklist is offered below for enterprise teams to use as they make this gradual transition. Obviously, different enterprise teams will have different present states, so their respective starting points will vary.

## SECURITY

- Have you enhanced your security policy rules to include use of public cloud services?
- Have you enhanced your security policy rules to include use of SaaS services?
- Have your security vendors shared their roadmap to cloud-based networking?

## NETWORK

- Have you reviewed your objectives to support cloud-based branch office networking?
- Have you reviewed your objectives to support increased work-from-home?
- Have you reviewed your objectives to support supplier and partner access?
- Have you checked that your business critical applications meet service-level agreements (SLAs) with shifts to the cloud?

## APPLICATIONS

- Have you inventoried and prioritized your business applications?
- Have you started roadmap planning to move legacy apps to the cloud?
- Have you reviewed any roadblocks such as regulations that complicate cloud app usage?

<sup>1</sup> East-West access is performed entirely within a defined perimeter, whereas so-called North-South access is performed across a perimeter (see Figure 2).

<sup>2</sup> Some analyst firms have created models such as Secure Access Service Edge (SASE) to define this new approach to secure networking with emphasis on the cloud.

<sup>3</sup> MPLS includes label headers on packets that are used for routing. The result of this label usage is separation versus additional security (as is commonly thought).

<sup>4</sup> Many commercial vendors will refer to this roadmap in the context of the SASE model.



# TAKE BACK CONTROL OF YOUR HYBRID WORK ENVIRONMENT

KATIE TEITLER

---

The past year's work-from-home operating environment caused a surge in cyber crime activity. Security and IT departments had to wrestle with securing formerly office-based employees in their homes. Even as personal and unmanaged devices were in use, employees were connecting often via insecure channels and/or fluctuating locations, and access rights were given preference over security control. As the pandemic winds down, businesses have a new challenge – securing hybrid environments where workers are fluctuating between on-site and remote locations, and are changing devices and geographies on a constant basis.

## INTRODUCTION

The COVID-19 pandemic caused a sudden and large-scale shift in how and where office-based employees work. While remote work and work-from-home were options for many employees pre-2020, at the start of 2020, working from home became a necessity for anyone with the ability to do so. The shift caused major initial disruptions and challenges for IT and security personnel. First, in the form of connectivity and access. Now, more than a year later, security teams are still grappling with how to handle the security of remote workers, their devices, and their access controls, especially when the issue of unmanaged devices comes into play.

While there is an end in sight for the pandemic, businesses and employees have now spent a year experiencing how remote work can be a boon to both parties, and it's unlikely that we will ever see a return to the in-office levels that dominated pre-pandemic. In other words, work-from-home and remote work are here to stay, in greater numbers, and with more flexibility than ever before. Pre-2020, it was common for businesses to operate with, perhaps, 20 to 30% remote and/or home-based employees. Beyond 2021, it is probable that the percentage of employees working in a hybrid remote model (i.e., part time in an office, part time in a remote environment) will double.

Now that the dust has settled on shifting business models to work-from-home, security teams are looking at long-term solutions to support hybrid work, with more people off site on a regular basis. However, with businesses offering employees the option of flexible work — meaning, part time work-from-home, part time in-office — the solution is not as simple as securing remote employees and their access requirements. Many employees will choose a hybrid arrangement, that is, some days working from the office and some days working remotely. In some cases, this will mean employees use different devices for each type of work. In every case, it will mean fluctuating types of assets touching the network, some of which are managed by the business, others that are not. It also means security teams need a fresh look at how users are connecting to corporate assets and resources and be able to adjust security policies to allow secure-but-easy access.

## A CHANGING ATTACK SURFACE

In this environment of hybrid work, employees are using a mixture of personal and business-supplied devices. The lines between personal and work have been blurred, and employees are more mobile than ever before. This will be even truer as the pandemic declines and employees return to coffee shops and public places to work and start traveling for business.

Employees will need secure methods of working, from wherever, whenever. Yet, as was true during the height of the pandemic and even at intervals before, they will rarely be onsite, on the corporate network. Securing employees' connections with old technologies like VPNs (which are becoming obsolete, due to the inherent bandwidth limitations and security threats) won't be an acceptable solution. As such, zero trust network access (ZTNA) has taken the place of outdated, kludgy connection technology, but zero trust is predicated on knowing every device and its security posture before validating the request.

Additionally, cloud now dominates corporate working environments. Cloud was originally proposed as a cost saver and scalability solution, but organizations cannot underplay the cloud's role in facilitating remote work and productivity. Its benefits are almost immeasurable. In the world of remote work, cloud is indispensable; it allows workers quick, easy, and secure access to the resources they need to accomplish their work.

That said, cloud is not without its security concerns. To start, IT and security teams don't always know

**“As such, zero trust network access (ZTNA) has taken the place of outdated, kludgy connection technology, but zero trust is predicated on knowing every device and its security posture before validating the request.”**

what cloud apps and services have been added, a.k.a., Shadow IT, which is a classic example of an asset management problem. Especially when cloud apps or services don't require special provisioning, security teams are unlikely to immediately notice when corporate assets are connecting to them. This is majorly concerning because cloud misconfigurations are emerging as a priority security threat; [research](#) suggests that 91 % of cloud deployments have at least one major exposure.

The attack surface is further expanded by the increase in cloud collaboration tools, which have shown themselves to be particularly useful when people are working in multiple, disparate locations. As these tools reside off-network, and employees can use non-work emails to access them, security teams may not be aware of them. Yet they pose a significant security risk when the data stored in them may be company-proprietary and/or if the devices touching them become infected and are then used to access other assets and resources.

## RISKS TO REMOTE WORK

In addition to the aforementioned cloud threatscape, in this section we will look at how cyber risk is increased by remote and hybrid work.

IT and security professionals have expressed concern (over the past year and during years prior to the pandemic as remote and work-from-home were gaining more traction) about the increased number of threats to businesses, resources, devices, and users when these assets cannot be secured in an on-network ecosystem. Some of those concerns include:

**Phishing:** Phishing remains a top threat vector which companies combat with the native anti-phishing/anti-spam built into their email clients and through supplemental anti-phishing, email, and endpoint controls. However, as every security professional knows, savvy phishers are able to evade detection and infected emails slip through controls all the time.

In a remote or hybrid work situation, the problems of preventing and detecting phishing are compounded; users toggle between managed and unmanaged devices, properly protected devices and personal devices with vulnerabilities, and varying working locations. Threat actors understand that the increase in entities organizations have to monitor and manage creates a resource challenge. They also understand that this increase makes it less likely that an organization will catch all the phish.

Further, less in-person interaction means more email, and more email means more phishing attempts. Even if a phish is aimed at a non-work device or account, if a user — or someone who has access to the user's device — clicks on a malicious link or downloads an infected attachment, and that user then uses the device for work-related purposes, the attack can spread and cause harm.

**Insecure Wi-Fi:** When employees are working remotely, there is no good way to control the type of network they're using to connect. In today's mobile world, blocking a device connecting via Starbucks or airport Wi-Fi, for instance, is productivity suicide. Businesses need to allow anytime, anywhere connectivity, but they need to do so in a secure fashion.

While outright blocking is generally not an option, real-time identification and management of what the device/user has access to goes a long way in preventing a breach. An understanding of how users are connecting to resources and an assessment of the level of risk the connection poses are baseline protection capabilities.

**Use of unsanctioned software:** When employees are working remotely, especially when using their personal devices, it is difficult to prevent them from accessing or installing unapproved software and applications. This is problematic from a security standpoint when the personal device is also used for work. Malicious software is highly prevalent, and the inability to track and control what's installed leaves organizations open to compromise. It's only through automated policy enforcement that companies can affect mitigation against connections from devices that contain malicious content.

**Unmanaged devices:** As more devices move offsite — both in number and type — tracking who's using which devices can be an asset management nightmare. This is especially true if the organization has to monitor every connection and manually configure every access request. Like with the challenges mentioned in previous sections, organizations cannot take a “just block” approach to managing unmanaged devices. It is counterproductive to how organizations operate. However, understanding the security hygiene and configuration of devices in use and then setting appropriate permissions mitigates cyber risk. This aligns with both a zero trust strategy and a strong asset management program.

**Shared devices/personal devices:** As with unmanaged devices, remote workers are apt to use personal devices, which may be shared with or accessed by unauthorized users. This could, potentially, result in unsafe apps being installed, malware infections, data leakage, unapproved access to data, and more. But again, simply blocking devices — even if they pose a greater risk — is not an option with remote and/or hybrid work. The key is understanding all the assets on or requesting access to your network, verifying their security state against policies, and automating policy enforcement.

**Remote desktop access:** In a world where more office-based workers are not on-site in a corporate office than are, remote desktop support has become indispensable. However, numerous attacks on RDP and remote IT and network management software — including the now-infamous SolarWinds Orion attack — have resulted in attacks against individuals and organizations. Since remote desktop will remain an important service for employees requiring technical assistance when working offsite, organizations need to ensure that unapproved, consumer-grade solutions aren't being used and that all connections between employees are configured properly. As misconfigurations are quickly becoming opportunities for cyber criminals to capitalize on, automating policy enforcement for every service is a must.

## MITIGATION FOR HYBRID ENVIRONMENTS

With a greater number of workers toggling between in-office and remote work environments (which, in and of themselves could vary based on employee preference), security and IT teams now face different challenges.

Automated asset management with policy enforcement can help with all of the above risk factors. It is therefore critical that organizations have a real-time monitoring and asset management plan for each device and device type requesting network and resource. A basic inventory is a good start, but ensuring policy enforcement across all devices, connections, and requests should be the baseline for risk control across your hybrid work environment. As such, organizations should seek a comprehensive asset management program and accompanying technology that includes:

- Comprehensive and accurate asset inventory and management
- Secure access management
- Application of consistent security policy enforcement across device types (managed or unmanaged)



## HOW CYBER SECURITY ASSET MANAGEMENT IMPROVES THE SECURITY OF HYBRID WORK

The network perimeter is a thing of the past, therefore it's no surprise that businesses did not, and will not, focus on the corporate network as the cyber security control point. The question now becomes: where is the new control plane? Some have argued that identity is the new perimeter. This makes sense, unless the definition of "identity" is relegated to human identity or a person using a device. In fact, in the digital realm, "identity" has always been a control factor for entities communicating on a network; digital device fingerprinting — i.e., gathering and tracking data about hardware and software — is not a new technique and has been used as the basis for many security tools over the years.

In addition, these newer technologies may employ deception to prevent impersonation. The idea behind this particular brand of deception is poisoning data sources — flooding identified malicious sites with false information like decoy credentials that seem legitimate but ultimately lead attackers to dead ends, thereby preventing account takeover. 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 take over accounts and steal data and information.

It is therefore a modern security requirement that enterprises understand the identity and security state of all deployed assets — human, software, and hardware — to properly secure them. Identity is a unique set of attributes for each asset, and companies can better understand and control their cyber security risk when "identity" is broadened to include all assets.

What complicates the problem of asset discovery, classification, and management (especially with hybrid work arrangements) is the increased numbers and types of assets in use in a typical corporate environment. As noted previously, most corporate employees admit to using multiple devices and/or personal devices when they work remotely. This not only increases the number of assets connecting into corporate resources, but the number of device types the business has to support from a security standpoint. And manufacturers don't make it easy; to date, no standard exists across ecosystems for either default settings or management of those settings.

When we look at system assets, like databases, cloud services, and software, remote work ushered in a new wave of resources dependent on complementary systems resources as well as new user access. Like with endpoint devices, the ability to gain visibility, management, and control vary based on asset. Thus, security teams must now create a strategy for how to handle onboarding and access to these assets. And the strategy has to accommodate a fluid workforce.

### ***It starts with visibility***

As cliché as it is to say, you cannot measure that which you cannot see. Cyber security asset management starts with an asset inventory. That means knowing every device type, every user, every application, every host, and every server in use. To adequately quantify the attack landscape,

**It is therefore a modern security requirement that enterprises understand the identity and security state of all deployed assets — human, software, and hardware — to properly secure them.**

discovering and identifying these assets must be continuous and in real time, especially for IoT and operational technology (OT) environments where assets might not be online and identifiable consistently.

Further, the inventory has to span network environments, given that most companies are operating some combination of multi-cloud, hybrid-cloud, on-premises, and virtual networking environments. Therefore, any asset management tool must work ubiquitously across environments and should, optimally, centralize asset visibility via one console.

Not only is it important to understand what assets are on corporate networks, but a complete asset inventory tool will include identification of how tools and systems are deployed and integrated. This allows security teams to ensure proper security and IT solution coverage, something that is very difficult and time-consuming without being able to view everything in one place.

## LESSONS LEARNED FROM SECURING A REMOTE WORKFORCE

The good news for secure remote connectivity at the start of the pandemic was that some organizations had already embraced hybrid work and had solutions and strategies in place — on average, businesses were running operating with 20–30% remote pre-2020. The bad news is that hybrid strategies weren't the case for the majority of organizations. Many businesses struggled to facilitate connectivity from remote locations and unmanaged devices, much less ensure the security and policy compliance of those devices.

Recommendations about asset inventory and management from CISOs we spoke about this challenge include:

- Start architecting (if you haven't already) for zero trust security. This will help with asset management.
- Use VDI and 2FA, thus allowing any BYOD; identification and policies then reside with the instance, making them easier to manage.
- For high-risk vendors and offshore contractor, install a corporate-generated certificate in addition to 2FA for an additional level of defense.
- Map asset management to frameworks, such as NIST 800-53 or CIS Controls, to prevent control gaps.

## EVALUATING CYBER SECURITY ASSET MANAGEMENT PLATFORMS FOR YOUR HYBRID WORKFORCE

An effective commercial cyber security asset management solution should allow businesses to identify all assets in real-time, regardless of their state, ownership, or location. Beyond basic asset inventory, customers will benefit from the ability to understand the security configuration of each deployed asset and align security policy requirements based on risk to the organization, compliance mandates, or vulnerability severity level when applicable.

With more employees working in and from remote locations, and with the high likelihood that hybrid work environments will become the corporate norm moving forward, security and IT teams need advanced solutions that go beyond real-time asset inventory. Modern asset management platforms add the ability for users to enforce policies and manage security solution coverage from a single console. They provide context and enrichment from third-party data sources, allowing users to quickly pinpoint relevant threat information. Further, users should execute remediation based on findings and allow admins to adjust policies and baselines based on cyber hygiene, validate required or desired

security policies, and close security gaps

When evaluating cyber security asset management platforms, the following questions will help determine which type of platform your organization needs:

- 1) *Risks* – How is your company currently assessing risk across in-office, home-based, and remote work?
  - a. *What processes and techniques are you using to identify cyber risk?*
  - b. *How are you estimating the scope of your attack landscape?*
  - c. *What/where is the greatest risk?*
    - I. Devices
    - II. Users
    - III. Access
    - IV. Software vulnerabilities v. Lack of visibility
    - VI. Lack of unified control vii. Other
  - d. *What is the business impact if attackers exploit critical assets?*
- 2) *Assets* – What types of assets do you maintain?
  - a. *How many and what types of assets does your company maintain (hardware devices, software, cloud, etc.)?*
    - i. What percentage are managed vs. unmanaged and/or personally owned?
  - b. *How are you tracking additions, updates, and changes to your assets?*
  - c. *How do you identify and validate security policy compliance for your assets?*
  - d. *How do you remediate asset vulnerabilities?*
    - i. What processes are used?
    - ii. What are the SLAs on remediation for “critical” and “high” vulnerabilities?

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

- 1) *Can the solution work ubiquitously across hybrid environments (i.e., on-prem networks, cloud, virtual, on-site, remote)?*
- 2) *How are asset inventories curated and maintained?*
  - a. How is data gathered?
  - b. Is data correlated and normalized to provide one single view into an asset?
  - c. How frequently are registries updated?
  - d. How does the platform handle unmanaged device identification?
- 3) *Does the platform provide management beyond asset inventory?*
  - a. Can you query security policies against which the platform can check for non-compliance?
  - b. Can the platform identify vulnerabilities such as missing patches, misconfigurations, and overly permissive access rights?
  - c. How easy/hard is it for administrators to write and deploy those policies?

d. Does the tool come with pre-built policy suggestions or playbooks?

4) *What remediation is possible when a vulnerability is found in an asset?*

a. How do users execute remediation—through the platform directly, or through third-party processes and/or tools?

b. Is any automation included?

c. How are remediations tracked?

5) *Deployment*

a. How is the platform deployed? Are agents or network scanners needed?

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

Outside factors have imposed severe restrictions on formerly-office-based work and caused yet another digital transformation, this time, in the form of remote work. As health factors improve and employees are able to consider a future where office-based work is once again tenable, both employees and businesses are rethinking a corporate world where 5-day-per-week in-office attendance is required for the majority of the workforce.

The evolution to hybrid work — where employees have flexibility to work in and outside of the office — offers great benefits. But it poses challenges to cyber security. First and foremost, security teams must wrap new processes, policies, and controls around assets, what- and wherever those assets may be and over any type of connection.

If identity is the new perimeter and zero trust (with its requirement to verify every device before access requests are granted) is becoming a baseline for security excellence, then it only stands to reason that organizations must have ongoing, real-time, accurate assessments of each and every asset in their ecosystem.

What's more, control can't stop at visibility; security teams must also incorporate methods to identify security policy coverage gaps, remediate non-compliance issues, and then enforce policy alignment. Optimally, the entire process is automated, making it easier for security and operations teams to manage the deluge of new assets and situations that will arise every day.

Cyber security asset management is a frequently overlooked element of cyber security programs, but in our new hybrid work world, it requires a fresh look.



# SECURING EMERGING 5G GLOBAL NETWORKS AND MOBILE INFRASTRUCTURE

EDWARD AMOROSO

---

Emerging 5G mobile infrastructure can be secured through the supply chain, core and radio network elements, virtual apps, mobile endpoints, carrier security programs, and quantum readiness. This report recommends how security protection in each area should proceed.

## INTRODUCTION

The emergence of 5G infrastructure around the world promises more service-oriented support for personal and enterprise use of mobility. Although increases in speed and capacity are welcome with 5G, the real power of this ongoing evolution from LTE to 5G comes from the flexibility of its underlying virtualization, as well as the extensibility of a more software-defined approach to mobile infrastructure.

5G infrastructure security cannot be analyzed based on one canonical architecture that will be in place everywhere. Rather, the transition to 5G will be stepwise, with many carriers opting for the Non-Stand Alone (NSA) mode of operation, where the existing LTE core network is used in conjunction with 5G radio. As a result, our analysis here must be somewhat broad to be generally applicable to the largest number of scenarios.

It is also worth mentioning that most 5G security compendiums have focused on how hackers might take advantage of specific usage scenarios such as texting over a 5G NSA architecture or making calls over a stand-alone architecture where the LTE core has been upgraded to 5G (see [1] for example). Such works are useful, but our attention here is broader, focusing instead on technology management initiatives.

With this in mind, included below are our recommendations for those areas of technology management that deserve the most intense focus to properly secure 5G infrastructure in support of personal and enterprise mobile usage. The intended audience includes those key decision makers regarding mobile security who reside within enterprise security teams, mobile carriers, standards groups, and applicable government agencies such as the National Institute for Standards and Technology (NIST).

The specific areas of focus for decision makers to ensure the highest levels of cyber security protection for 5G infrastructure include the following:

- **Supply Chain** – Developing rational supply chain policies for selection of 5G vendors is an essential component of any enterprise or carrier mobility security program. This area deserves primary attention by business leaders and government decision makers. The goal should be rational policy for secure supply chain management in 5G.
- **Core and Radio Network** – The internal configuration, including cryptographic controls, of 5G architectures must be assessed in the context of local security requirements. This area deserves primary attention from mobile carrier leadership. The goal should be an optimally secure 5G infrastructure for business and personal use.
- **Virtual Applications** – Since 5G introduces a service-based architecture (SBA) to mobility, extensibility via software applications must be properly secured. This area must be addressed by the app development community in conjunction with mobile carriers. The goal should be the most secure integrated 5G environment for delivering apps.
- **Mobile Endpoints** – With emerging emphasis on zero trust security, cooperative protection between 5G-enabled devices and the network will be imperative. This area must be focused on between device OEMs and mobile carriers. The goal should be to optimize integrated security protections between devices and 5G infrastructure.
- **Carrier Security Programs** – Because 5G will play such a central role in emerging services, carriers will play a more central role in end-to-end security. This area must be coordinated between the mobile carriers and business leaders. The goal should be to ensure that carriers are stopping all attacks, including the most advanced.
- **Quantum Readiness** – 5G infrastructure will be in place for a longer time than previous generation networks, so it will be in place as quantum computing becomes mainstream and quantum threats emerge. This area must be coordinated primarily by the mobile carriers. The goal should be a practical, quantum-proof security strategy and plan for evolving 5G infrastructure and preparations should start now.

5G Area of Focus	Key Decision Makers	Goal
Supply Chain	Business and Government Leaders	Rational supply chain security strategy
Core and Radio Network	Mobile Carriers	Optimally secure 5G infrastructure
Virtual Applications	Developers and Mobile Carriers	Integrated support for 5G apps
Mobile Endpoints	OEMs and Mobile Carriers	Security integration of 5G devices
Carrier Security Programs	Mobile Carriers and Business	Highly secure carrier options
Quantum Readiness	Mobile Carriers	Rational plan for quantum threat to 5G

**Figure 1. Most Important Areas of Focus for Decision-Makers in 5G Security**

The sections below address the relevant technical and management issues for each area, along with our recommendations for reducing cyber risks in emerging global 5G infrastructure. The guidance targets key decision makers, but anyone involved in any aspect of 5G infrastructure design, development, delivery, operation, use, dependency, or assessment will hopefully find value in the recommendations.

## SUPPLY CHAIN

It should come as no surprise that supply chain issues play an important role in the design, implementation, and selection of 5G mobile infrastructure. Perhaps less obvious is that such attention to supply chain for security must expand beyond the familiar debates around country-of-origin for mobile components. Rather, a holistic supply chain plan must take into account all suppliers of a given 5G implementation.

The specific threat vector associated with supply chain security in 5G infrastructure involves equipment and software vendors inserting hidden and unknown Trojan Horse code into their products. The goal would be for the vendor, presumably with involvement of its sponsoring national government, to collect information traversing the network, or to disrupt operations as part of a malicious or even military campaign against the 5G hosting country.

Unfortunately, the individuals and groups who make decisions regarding supply chain security for 5G networks do not include the majority of users who depend on this infrastructure. Instead, these decisions are made by those entities with responsibility to either build, operate, or legislate the use of 5G in a given country or region. The specific decision makers for 5G security, and recommendations on how they should address this issue, are listed below:

- **5G Mobile Carriers** – The decision about which vendors to use in 5G infrastructure is ultimately made by the carriers. This should be done with the goal of providing the best possible (and most secure) experience for end users.
- **Federal Government** – Supply chain input from any federal government should calmly and accurately emphasize the security of 5G mobile infrastructure rather than any political purposes that might change over time.
- **End Users** – The individuals and groups dependent on 5G infrastructure should make their voices heard regarding the types of supply chain decisions carriers are implementing in their mobile services.

The canonical example of supply chain decision making for 5G is the debate within the United States around whether to include Huawei equipment in emerging mobile infrastructure. Setting aside the specifics of that debate, it is worth acknowledging that this Huawei-related issue has become distinctly political in the U.S. This is unfortunate, because it muddles the rational threat-based considerations that carriers should be performing.

In contrast, the UK government has been managing a group called the Huawei Cyber Security Evaluation Centre (HCSEC) [2]. The HCSEC has been weighing and managing supply chain decisions regarding use of Huawei in UK-based infrastructure for many years. Their decisions have been based on an engineering analysis of the pros and cons of using Huawei equipment, rather than superficial analysis based on political debate.

## CORE AND RADIO NETWORK

While 5G infrastructure is inherently complex, it also must address complicated hybrid arrangements including SBA mode, where the legacy core remains. In such configurations, 5G radio access is connected across standard 4G/LTE interfaces. This hybrid approach implies that security engineers must carefully attend to any threat-related design issues that can arise in the subtle interactions between the mobile core and the radio network.

One significant mobile security issue is that configurations can exist in specific 5G carrier infrastructure where the important interface (referred to by engineers as S1-U) between the radio access portion of the network and the mobility core might not be encrypted. The emerging 5G standard relaxes this requirement under certain circumstances, presumably to allow carriers to maintain high levels of performance for mobile users.

	Security Threats Caused by Unencrypted S1-U Link	Security Threats Unrelated to Unencrypted S1-U Link
<b>Confidentiality – Data Exfiltration</b>	✓ (Encryption prevents exfiltration)	
<b>Confidentiality – Local Exposure</b>	✓ (Encryption prevents exposure)	
<b>Integrity – Man-in-the-Middle</b>	✓ (Encryption prevents MitM)	
Integrity – Data Corruption		✓ (Encryption doesn't prevent corruption)
Availability – Transmit Delay		✓ (Encryption doesn't prevent delays)
Availability – Denial of Service		✓ (Encryption doesn't prevent DOS)

**Figure 2. Threats Introduced by Unencrypted S1-U Interface**

The challenge for users of 5G infrastructure is that except for the most advanced and informed users of mobility (such as large government organizations), the existence of core or radio network security weaknesses will not be known. This implies that prominent voices must demand that mobile infrastructure be scrutinized by experts and that their findings be made public. Important aspects of this process include the following:

- **Infrastructure Visibility** – The 5G systems supporting the emerging mobile infrastructure must be designed to provide sufficient telemetry for real-time visibility into operations. This is critically important for proper cyber security of mobile networks.
- **Framework Compliance** – Enterprise users of 5G mobile services will be obligated to demonstrate compliance of their infrastructure with frameworks such as the NIST Cybersecurity Framework. 5G carriers must effectively support this activity.
- **Real-Time Flexibility** – The software-defined aspect of 5G infrastructure should enable more flexible operation, including real-time enhancements and live adjustments of security defenses to mitigate ongoing attacks (e.g., for DDOS security).

Admittedly, most personal and business users of 5G mobile services will have no idea of the security aspects of their carrier's offerings. It falls to expert teams, oversight groups, prominent enterprise users, and government regulators to ensure that the core and radio network support for 5G mobile infrastructure is properly secured. This should be a continual and ongoing process for as long as these new mobile services are in operation.

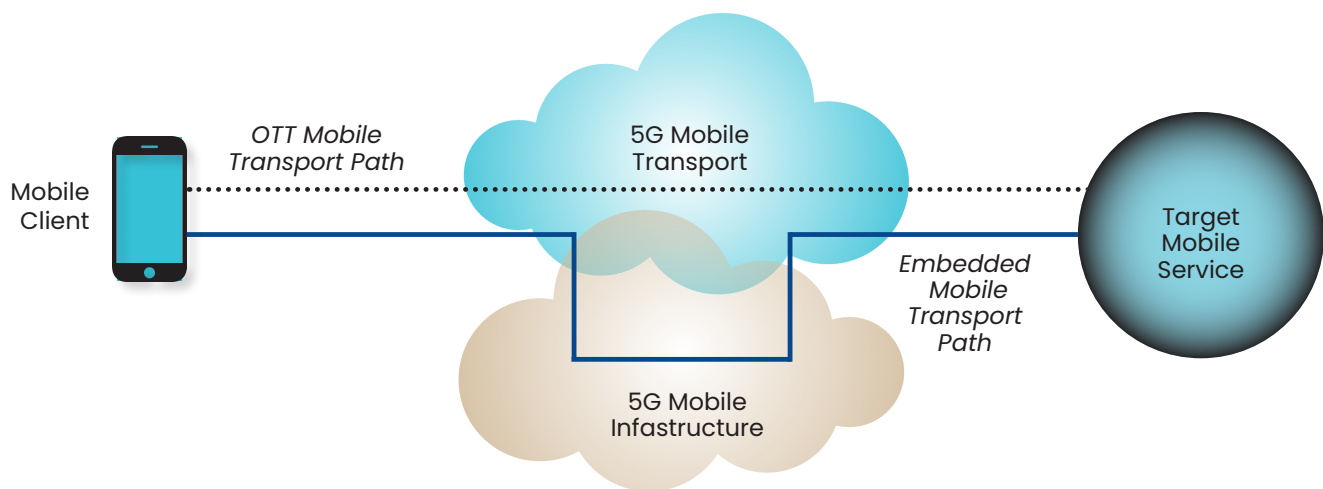


## VIRTUAL APPLICATIONS

Unlike previous generations of mobile infrastructure such as 3G/UMTS and 4G/LTE, the emergence of 5G mobility is software-based. As such it introduces a service-based architecture (SBA) that will allow for effective support of virtual applications. These might exist on the mobile device, in public or hybrid cloud, or directly in the mobile core network on the northbound interface of a software defined network (SDN) controller device.

To understand how a carrier network can support different services requires that one recognize the difference between over-the-top (OTT) applications and embedded mobile network core functions. The most common OTT applications are designed to operate independently of the underlying network infrastructure implementation. They are often said to run over a network, versus within – hence the OTT designation.

In contrast, applications that are supported within a network core are built to take full advantage of the internal design elements of the carrier infrastructure. A reasonable example is the native SMS (short message service) texting capabilities offered by mobile carriers, which ride within their telecommunication service – versus the use of Apple’s instant message service (iMessage) which rides over any type of network including WiFi.



**Figure 3. OTT versus Network-Embedded Services**

This software orientation provides great advantages for 5G mobile infrastructure providers. The expansive flexibility afforded any software-defined system allows for the rapid introduction of new services for customers. It also creates the opportunity for the 5G infrastructure to be fine-tuned or adjusted to internal or external conditions. The following advantages emerge for any operators or users of 5G services:

- **Embedded Services** – The potential to create more embedded, network-based services is a great advantage of emerging 5G. While OTT services will work well over 5G network infrastructure, embedded services offer a stable and highly secure option.
- **Rapid Threat Adjustment** – The flexibility inherent in software-oriented, service-based infrastructure is that changes can be made quickly. This allows for dynamic defensive adjustments to mobile infrastructure based on real-time threat conditions.

- **User Requirements Tailoring** – The software orientation of 5G infrastructure will allow carriers to support the unique functional requirements of important users more readily since new hardware will typically not be required.

## MOBILE ENDPOINTS

Modern enterprise security encourages lesser dependence on firewall perimeters with greater focus on open, internet-based zero trust network access (ZTNA) to cloud-hosted workloads. Much of this access will be accomplished directly from the device to the application using mobile-connected endpoints over 5G mobile infrastructure. This underscores why mobile endpoints must coordinate security with the 5G network.

An extension to the endpoint space in the context of 5G infrastructure involves Internet of Things (IoT) and related Industrial Control System (ICS) devices that will require mobile access. This increases the overall value of emerging 5G infrastructure, especially since the new network services are being designed to include support for new applications, including ICS-based systems that might include machine-to-machine operation.

Enterprise and personal users of mobile services will benefit from the improved and more integrated support offered by emerging 5G infrastructure for mobile endpoints. Much of this comes from the flexibility in software-defined 5G infrastructure, as well as the attention to functional extensibility during 5G design. 5G users should expect to see value in the following areas:

- **IoT Device Support** – Non-PC devices will create new challenges for security teams in the context of 5G. Appliances, cars, homes, medical systems, and other devices do not, for example, include obvious risk reductive measures such as patching support.
- **ICS System Support** – The connection of ICS infrastructure to 5G networks will require additional security controls, especially to address the risk from nation-state actors who are intent on targeting their adversaries.
- **Programmable Device Security** – 5G systems can be programmed to tailor security support to special devices because the support infrastructure is software-based and more easily adjusted to the security needs of endpoints.

## CARRIER SECURITY PROGRAMS

While 5G mobility will further enable decentralized work-from-home by employees and will serve to untether citizens from the need for WiFi hotspots for connectivity, it also introduces more centralized dependence on the mobile telecommunications carriers to prevent threats. The effectiveness of mobile carrier security programs will become an important concern and critical business driver for 5G mobility buyers and users.

Threat discussions often gravitate toward this increased dependence on the carrier, often citing concerns about a more targeted risk. If the carrier is hacked, then the consequences can be significant. While this is a fair assessment, distributed network security over the past two decades has shown that most organizations are not up to the task of properly protecting their assets from cyber attacks.

The implication is that by putting more 5G security eggs into one basket (so to speak), some additional risk emerges with the more centralized target. At the same time, however, if the carriers are better suited to the task of protecting enterprise assets, then the overall effect on risk will be mostly positive. This will be true for nation-state risks that can only be countered by experienced teams – and carriers tend to have well-funded defenses in the following ways:

- **Centralized Mobile Defense** – The mobile carriers will have to ensure that their more centralized security support for 5G is properly coordinated, and this is likely since carriers have tended to have some of the best security programs in the world.
- **Well-Trained Mobile Security Teams** – Attracting and maintaining the most capable and educated security experts in the world is a reasonable goal for well-funded 5G security teams within mobile carriers.
- **Cooperation Across Mobile Telecom Sector** – The 5G community will have to ensure a reasonable level of coordinate and cooperation as global infrastructure becomes more dependent on their emerging 5G systems.

## QUANTUM READINESS

The flexible, adaptable, and extensible nature of a 5G software-oriented architecture will allow the infrastructure to remain in place far longer than its predecessors. It is reasonable to assume that 5G will carry the global community into the era of quantum computing and its corresponding security threat, when quantum computing will have the potential to break the encryption on which most enterprises, digital infrastructures, and economies rely.

To address the threat to organizations and 5G networks posed by quantum computers, organizations will have to take inventory of their existing cryptography and data security requirements and start developing an end-to-end strategy to identify and mitigate any weaknesses or risk. At the same time, they must demand cryptographic strengths required from their 5G provider for data in motion.

5G standards must address the quantum threat and support the development of alternatives to public key infrastructure (PKI) ciphers. Organizations, governing bodies, and carriers should recognize that all forms of quantum-safe security have unique merits and limitations and as a consequence, cyber security best practices dictate the use of multiple forms and layers of protection known commonly as defense-in-depth.

5G ecosystem participants are strongly encouraged to adopt a posture of quantum readiness and defense-in-depth countermeasures to address the challenges that quantum computers will pose. A focus on crypto-agility will enable 5G network providers to deploy quantum-safe alternatives in advance of the emergence of quantum computing and to adjust to threats as they develop.

This work should include attention to emerging post-quantum cryptographic (PQC) algorithms as preferred alternatives to existing PKI-based systems, as well as considerations to new technologies including physics-based Quantum Key Distribution (QKD) for ultra-secure communications.

To effectively mitigate the expected threat from quantum-based attacks, enterprise teams and mobile carriers should adopt a cyber-agile posture enabling them to craft the best cyber security solution for their unique needs from the widest range and combinations of quantum-safe solutions.

In 2016, NIST warned that all organizations should start preparing now for the coming quantum cryptography break. 5G mobile carriers, federal government, and end users must heed that advice today to prepare their organizations for the quantum security threat. For each, the following steps and considerations should be taken now to ensure their organizations and the emerging 5G infrastructure are ready for the quantum age:

- Conduct a data protection inventory and quantum risk assessment
- Practice crypto agility and deploy a mix of classic and quantum-safe crypto
- Build a dynamic quantum infrastructure that can easily keep pace with change
- Implement candidate PQC algorithms
- Encrypt critical data with quantum keys
- Leverage QKD for maximum security.

## References

[1] M. Bartock, J. Cichonski, and M. Souppaya, *5G Cybersecurity: Preparing a Secure Evolution to 5G*, NIST National Cybersecurity Center of Excellence, Draft – February 2020.

[2] Huawei Cyber Security Evaluation Centre Oversight Board. *Annual Report 2019*  
[bit.ly/2TLVIYv](https://bit.ly/2TLVIYv)



# WHAT EVERY CISO SHOULD KNOW ABOUT INSIDER THREATS: AN FAQ AND SECURITY CHECKLIST FOR CISOS

KATIE TEITLER

---

Insider threat management is a challenging topic, both from a human aspect as well as a technological aspect. Chief Information Security Officers (CISOs) walk a fine line: they must ensure their organizations are free from malicious or accidental harm, but they also need to allow people access to authorized resources. In this report, we explore the complexities of achieving two seemingly polarized goals and explain how CISOs and their teams can accomplish effective insider threat management from a people-centric perspective.

## INTRODUCTION

To establish an effective insider threat management program, you need to understand what an insider threat is and why insider threats matter.

Simply, “insider threat” is a term that connotes the potential harm a person with authorized permissions and access to organizational resources can cause, either purposefully or by accident. The use cases for insider threat are plentiful and varied, ranging from a disgruntled worker who intentionally steals company secrets or sabotages systems to a well-meaning employee who accidentally deletes files or copies data to an insecure device, thereby introducing the opportunity for a threat actor to socially engineer user credentials to execute data theft.

This summary starts to shed light on why insider threats matter. CISOs and their teams need to understand what drives and facilitates insider threats, as well as the impact of an insider threat. It's only when equipped with this greater understanding that CISOs can effectively mitigate insider threats.

## DRIVING FACTORS FOR INSIDER THREATS

According to the 2020 Ponemon Institute Cost of Insider Threats report, insider-driven cyber security incidents have increased 47% since 2018. The five main causes of this dramatic increase include:

- **Expanded ecosystems:** Due to the highly interconnected nature of technologies, systems and services, partners, contractors, vendors, and suppliers all need a certain level of access to corporate resources. That number exponentially increases when adding in the number of partners, contractors, suppliers, etc. to which your third parties are digitally connected. The supply chain effect of an insecure Nth party means that insider risk extends to everyone and everything that can pivot through technology to compromise a company.
- **Hybrid work:** Formerly office-based organizations now have to support highly fluctuating work environments, with some workers onsite, some remote, and some toggling between the two while frequently changing devices and connectivity methods. Traditional approaches to perimeter and endpoint security no longer apply, leaving organizations unprepared, unprotected, and susceptible to insider threat.
- **Cloud-based collaboration tools:** Part of the expanded ecosystem of digital resources includes the use of cloud and collaboration technologies. These tools expand the attack surface and present new and numerous options for accidental and malicious data compromise, especially because controlling access is a major challenge when dealing with resources that are specifically designed for ease-of-use and efficiency.
- **Always on connectivity:** With the ubiquity of smartphones (a.k.a., minicomputers carried at all times), people can access work resources at any time, from anywhere. The pressure to do so can lead to fatigue, additional stress, and frustration with the organization, all of which increase the risk of insider threat. Further, because most workers use personal devices for work purposes, organizations cannot easily control the security hygiene of the devices connecting to corporate resources. This leaves them more vulnerable to exploit.
- **Job-related stress:** In a tight job market, workers feel great pressure to perform to the highest standard, even if it means sacrificing personal lives and interests. Today's workforce faces job insecurity, caregiving interruptions during the day, and monotonous work schedules, among other things, thereby increasing the risk of insider threat.

These elements equal tremendous risk, but this list is far from exhaustive. There are as many use cases and causes of insider threat as there are insiders. This means that anyone connected to an organization, whether they're a traditional insider (i.e., employee) or other third party, could be an insider

**“Effective insider threat reduction is people-centric security with an emphasis on technological solutions that allow for layered controls and real-time behavioral monitoring.”**

threat risk. Therefore, to handle insider threats and mitigate risk, enterprise security teams have to devise new processes and techniques.

The key to insider threat management is people. But before skepticism sets in, don't think this paper is going to focus on basic security and awareness training. It is true that employees need to be aware of cyber threats, like phishing and password hygiene, but any security professional knows that awareness – and even improved user actions – are not enough, especially in the case of maliciousness. There isn't enough training in the world to stop a motivated insider with authorized access to system resources.

True insider threat reduction requires the use of advanced technology that focuses on people, behaviors, and hardened policies for access controls and data. These features allow security teams to unearth and prevent insider threats while meeting privacy requirements and cyber security compliance.

Effective insider threat reduction is people-centric security with an emphasis on technological solutions that allow for layered controls and real-time behavioral monitoring.

## FREQUENTLY ASKED QUESTIONS

Here is a list of the common questions around insider risk management and how to implement an effective program.

### What is an “insider”?

As previously mentioned, an “insider” is more than an employee, contractor, or other human with direct access to corporate systems and data. Vendors, suppliers, and partners may have direct or indirect access to systems and data. Think about the type of access your payroll provider might need – employee name, address, W2 information, bank account information, email address, and social security number, to name a few. That's a lot of private and sensitive information to which legitimate non-employee, i.e., “insider” users, have access.

### Are there different types of insider threats?

There are three primary types of insider threats: malicious insiders, compromised insiders, and accidental insiders.

#### **Malicious insiders**

Based on the coupling of the term “threat” with “insider;” it's not unreasonable to default to the notion that insider threats are mostly malicious. While these can be some of the most insidious threats based on the fact that they are generally carefully planned and constructed, malicious or intentional insider compromises only make up about 23% of all insider threats.

Malicious threats often take the form of revenge or personal gain. For instance, an employee who feels they have been wronged by the company may extract revenge by stealing or destroying data, and perhaps even selling it to a third party. A malicious insider can also simply be someone who feels entitled to sensitive data or intellectual property. For instance, a salesperson who built up a virtual Rolodex of customers while working at the company may believe they have the right to copy that list when they leave.

#### **Compromised insiders**

Social engineering and phishing, in particular, continue to be the most reliable ways threat actors gain unauthorized access to organizations' systems and data. When a threat actor manages to gain legitimate access, either by tricking a user into handing over credentials or by buying credential dumps

from illegal forums, they can move stealthily through the organization's infrastructure. In many cases, the user does not know they've been compromised, and security teams must rely on behavioral analysis to identify threats.

A compromised insider may also be someone who was "turned" by a bad actor who uses threats to coerce the insider into inappropriate behavior.

### **Accidental insiders**

The reality is that most insider threats are caused by well-meaning people trying to do their jobs. Sixty-two percent of insider threats are caused by legitimate, authorized users. Examples may include an employee who copies data to a file share so they can work on a project outside of the office, but the file share is consumer grade, doesn't have the correct access permissions configured, and a threat actor gains access.

An accidental insider might also be a marketing team that deploys a SaaS marketing solution that is not configured correctly and leaks customer data, a user who installs an unapproved application that steals or leaks data, or a person who loses a device with sensitive information stored on it.

## **WHAT IS THE PREVALENCE OF INSIDER THREATS?**

Incidents on the rise. There has been a 47% increase since 2018 and the cost of insider threats is approximately \$11.45 million per incident. The impact of insider attacks is not limited to financial loss; additional ramifications include data loss, operation disruption, brand damage, loss of customers, loss of revenue, and compliance fines, to name a few.

Insider threats can be tricky to identify, especially in the case of compromised users. Possible warning signs that could imply someone has been compromised include:

- Accessing/copying/exfiltrating large amounts of data
- Attempting access to never-before-used databases/requesting access to data/systems not related to their job function
- Attempting to bypass security
- Violating company security and privacy policies
- Unusual changes to account permissions
- Inappropriate social media chatter
- Inappropriate system use

## **HOW CAN YOU COMBAT AGAINST INSIDER THREATS?**

The key to combating insider threats is people-centric technology and processes. Solutions must correlate user activity and data movement to calculate user risk. For example, one anomaly or activity does not constitute insider risk. Systems must be able to build profiles and

**“Sixty-two percent of insider threats are caused by legitimate, authorized users.”**

**“The impact of insider attacks is not limited to financial loss; additional ramifications include data loss, operation disruption, brand damage, loss of customers, loss of revenue, and compliance fines, to name a few.”**



timelines, and monitor for unusual data or system requests, abnormally high data exfiltration, privilege abuse, unintentionally risky actions, and policy abuse.

In a privacy-centric world, platforms should incorporate data masking and/or anonymization, strong data security, customizable data exclusion policies, zero trust-based access controls, and comprehensive auditing.

Clearly, this illustrates a need for platforms to work ubiquitously across on-prem, cloud, and virtual environments, and be able to correlate telemetry from disparate systems. Additionally, it's vital to enrich telemetry with behavioral profiles and threat intelligence. This allows for the behaviors of high-risk employees, like executives and disgruntled employees, to be prioritized. Leveraging a dashboard, similar to Proofpoint's Insider Threat Management dashboard (below), offers a quick view into the activities happening across the organization, ensuring the CISO and their team can effectively monitor insider behaviors and respond accordingly.

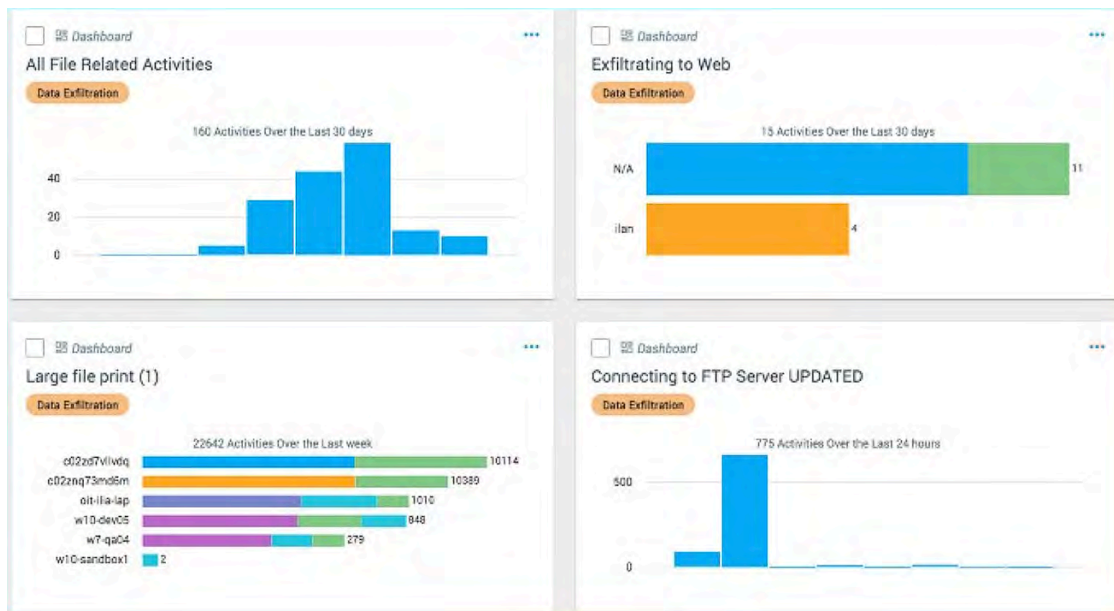


Figure 1: Proofpoint Insider Threat Management dashboard

## THE ROLE OF AN INSIDER THREAT MANAGEMENT PLATFORM

An unintentional consequence of the rapid shift to a work-from-anywhere world is that it created new opportunities for insider-led breaches. Here is a look at the top used alerts from Proofpoint's Insider Threat Management during the COVID-19 pandemic when the world shifted to a remote work environment.

As you'll note, many of these activities point to potential accidental insider threats, such as connecting unlisted USB devices, opening a clear text file that could store passwords or downloading a file with a potentially malicious extension.

### Top 10 Insider Threat Management Alerts

RANK	ALERT	Change from 2019 (Pre-COVID period)
1	Connecting unlisted USB device	▲ 1
2	Performing large file or folder copy	▲ 7
3	Exfiltrating tracked file to the web by uploading	▼ 2
4	Opening a clear text file that potentially stores passwords	▲ 1
5	Downloading file with potentially malicious extension	▼ 2
6	Performing large file or folder copy during irregular hours	▲ 4
7	Exfiltrating a file to an unlisted USB device	▼ 3
8	Installing hacking or spoofing tools	▼ 1
9	Accessing upload and sharing cloud services	▲ 6
10	Opening agent folder	▲ 4

These seemingly harmless actions are exactly why accidental insiders comprise 62% of insider threats.

**Figure 2: Top Security Alerts from the Work-from-home Period**

## YOUR CHECKLIST FOR EVALUATING INSIDER THREAT MANAGEMENT PLATFORMS

When evaluating insider risk mitigation solutions, the type of questions to ask fall in one of two buckets: risk and technology. The following questions will help determine which type of platform your organization needs:

1) *Risk – How is your company currently identifying employees, partners, and customers who pose a potential threat?*

- *Do you maintain acceptable use policies?*
- *How do you handle identifying and reporting of suspicious behavior?*
- *How are you assessing people for security awareness?*
- *What are the potential ramifications of an insider-centric compromise?*
- *How long would it take your company to recover from various compromises?*
  - *Data theft?*
  - *Data destruction?*
  - *Ransomware?*
  - *System disruption?*
- *What privacy standards and security regulations must your organization comply with?*

- 2) *Technology- What processes and technologies for insider threat monitoring do you maintain?*
- How do these tools/processes identify insider threats?*
  - What indicators are they monitoring?*
  - Are they endpoint or data focused?*
  - Is/how are sensitive data and systems classified?*
  - Can your deployed tools provide holistic visibility across endpoints, applications, data, browser usage, etc.?*
  - Do your tools provide the ability to build threat profiles and attack timelines?*
  - Do they allow your team to create visualizations of attack and conduct forensic investigations?*
  - Do you have the capability to stop an in-process incident?*
  - How easy are they to tune when baselines change (e.g., at the beginning of the pandemic when use and behaviors had to change drastically in a short period)?*
  - How do these platforms handle personal privacy versus the needs for insider threat monitoring?*
  - How easy/hard is it to map your technologies against compliance mandates, industry standards, and frameworks?*
  - How easily does your insider threat management platform integrate with complementary technologies, like SIEM and SOAR?*

## CONCLUSION

Insider-driven cyber security incidents have increased 47% since 2018. It's only fair to assume this number will rise as a result of the proliferation of our work-from-everywhere world and the increasing reliance on the supply chain. Implementing an effective threat management program requires a combination of people-centric security with an emphasis on technology and processes. Doing so allows security teams to establish strong access controls and focus on people and behaviors, all while meeting privacy requirements and cyber security compliance.

# INVESTIGATING DATA-CENTRIC SECURITY STRATEGIES

ADAM LEWINTER

---

Data is the life blood of most enterprises which has quickly led it to become the most valuable asset within the enterprise. As data architectures have continued to evolve and grow in complexity, security is often left behind. A data-centric security strategy will be a key for the success of all enterprises.

The amount of data generated and stored in an enterprise environment continues to grow at exponential rates. Users interact with numerous applications and websites that collect their personal data daily—legal names, home addresses, credit card information, etc. The amount of data collected is likely to continue to grow as internet connected devices become more prevalent in daily life and gather even more data about the behaviors and preferences of users.

However, it is not just end user data that is driving the overall growth. Previously analog systems have quickly transformed into digital systems that provide data critical to an enterprise maintaining a competitive advantage or the stability of a service. Inventory management, production line telemetry, and industrial controls have all increased the amount of data generated that is crucial to ensuring functioning environments.

Further complicating the situation, as application and website architectures have continued to evolve, they have become more interconnected with other internal and external applications, providing more avenues of access to the sensitive information. The continued adoption of APIs has also increased the exposure of data as they make sharing data even easier. In modern applications, when data is acquired by one company it is often shared with many which only adds to the complexity of developing a security strategy to protect it.

The amount and speed at which data is collected in modern environments has quickly overwhelmed most security teams' strategies to protect it. Security teams



are also no longer the key holders to deploying a new, secure database. Application owners, database administrators, and developers now have the power to simply “spin up” databases as they need to. The data stores exist on-premises as well as in cloud environments and are accessed by internal and external applications. With all these challenges, enterprise security teams struggle to distinguish malicious data access from legitimate data access in large part because they do not have a clear understanding of all access pathways to data. It is therefore paramount that modern data security strategies provide visibility and context at each stage along all pathways to the data and place security controls as close to the data as possible. As environments continue to shift towards being defined by data rather than by the individual applications, the visibility and context provided by data security solutions will be key for the success of an enterprise.

## UBIQUITY OF DATA

Since the explosion of the big data movement circa 2005, technological advances have allowed enterprises to collect and process more data than ever before. Mobile applications, websites, and smart devices all report telemetry back about the user and can often contain sensitive information. Production line automation and industrial systems are controlled by the data reported back from embedded sensors and software. This telemetry data is the life blood of most enterprises and has caused data to quickly become the most valuable asset within the enterprise.

However, there is a serious issue with collecting data at this scale—storage for this volume of data is expensive. While the unit cost for storage has continued to decrease over the past decade, the increase in volume of data has canceled out any savings and led to cost becoming an issue. This means most enterprises store the collected data wherever it is most cost-effective to do so, and this means enterprises have numerous data stores in numerous locations. This is an issue for security teams as each data storage technology has its own unique properties and exhaustively defining pathways and access behaviors to these data stores is a near impossible task.

Further compounding the problem is that the data is constantly moving. Since the data is stored where it is most cost efficient, it is often the case that the data requested to perform a certain analysis needs to be pulled from multiple locations. This means there are myriad pathways open between data store locations and applications, and more are created as demanded by new analysis needs. The increase in use of APIs in modern architectures as a vehicle to share data has greatly improved internal and external collaboration, but the ease of implementation means APIs are constantly in flux as they are frequently created or updated. This moving target makes it even harder for enterprise security teams to get the accurate understanding of the current state of an environment required to develop a strategy to secure the data that is passing through.

## BRING SECURITY TO THE DATA

The solution to securing the dynamic and highly connected world of data collaboration is to bring controls to the data itself. Complex pathways mean traditional controls implemented at the network or application layer are quickly becoming inadequate. Without a single point through which all requests flow, these traditional tools leave blind spots. Bringing controls directly to the data removes the dependency on the transport mechanisms and means that sensitive information can be protected even when not all paths to it are known. The natural place to put these controls is at the data store.

Database security has traditionally been focused on compliance. Database activity monitoring (DAM) solutions are designed with compliance in mind and understand what to look for because the result to be achieved is well defined by the regulations. These solutions discover and classify data that is then compared to policies to see if compliance regulations are being adhered to. They also provided audit trails and basic analytic capabilities to alert when anomalous access is detected.

DAM solutions are a strong foundation for any data security program, but most enterprise teams use them just for monitoring. Monitoring is of course crucial for visibility, but the value of the insights is diminished if they cannot be combined and correlated with other aspects of the environment. APIs and internal and external collaboration have added many more complex interactions with data that monitoring alone cannot fully understand and analyze.

Monitoring strategies also quickly become inadequate when shifting from a compliance to a security mindset. Rather than comparing the current state of a data store to a known list of requirements, enterprise security teams are now tasked with looking for the unknown, zero-day security threats. Just like with any security journey into the unknown, visibility and context is key. Critically, the context must also include information for all the stages in the pathways that lead to the data store as well as the relationships with downstream and upstream activities at each stage in the pathway.

## BEYOND MONITORING

Data security has followed a traditional evolution of maturity. DAM solutions support teams in their compliance efforts to make sure regulatory standards are being met. DAM solutions work well in traditional environments where data requests are ultimately funneled through a set few applications or servers. In these environments, DAM solutions are effective because they have an exhaustive view of data access and don't have to worry about numerous other pathways to the data.

However, the shift to a more data-centric view has brought data closer to the edge and exposed many nontraditional pathways which makes determining enforcement points difficult. Modern architectures that take advantage of technologies offered by the cloud such as the ephemeral nature of containers or the high connectivity of mesh networks create pathways to data that previously did not exist. Traditional DAM solutions struggle to account for these new pathways as they can only see the data access that flows through them and integrating the solution into the numerous data storage technology now available is a real challenge.

In addition, as data security needs mature, requirements around risk management capabilities have emerged that enable teams to make risk-based decisions around the storage of sensitive information in different locations. Data privacy continues to be at the top of the minds of end users as data breaches continue to be in news headlines. Data security strategies now have more complex requirements and considerations that DAM solutions are not built to handle. The next generation of data security strategies need to account for the changes in architecture and privacy requirements.

## REQUIREMENTS FOR A DATA-CENTRIC SECURITY SOLUTION

1. *Native cloud integration is paramount*

As the adoption of cloud technologies continues to increase many enterprises are no longer limiting themselves to a small set of technologies. It is not uncommon for each application within an enterprise to have a completely unique technology stack which means a data-centric security solution should be able to integrate natively with the cloud technologies to collect the visibility and context needed without conflicting with other technologies. Providing a normalized view across the disparate technology stacks is the first key requirement to being able to secure the data in enterprise environments.

## 2. *Embrace Zero Trust principles*

The second key requirement is embracing zero trust principles. A data-centric security solution should move away from overprovisioning access at the data storage tier and instead define dynamic policies based on who should have access to the data and what actions they should be able to take on a per event basis. Defining policies such that there is a set window of time in which certain actions can be taken by specific people will allow users to get the data required without overexposure and without the risk of forgetting to clean up temporary access permissions. This adds another direct layer of access control at the data store tier to define what users can do.

## 3. *Intelligent analytics must be built in by default*

The third key requirement is that data-centric security solutions should perform their own behavior and entity analytics without reliance on 3rd party tools such as a SIEM. Traditionally, attempts to secure data have been reliant on network event correlation, but these efforts often fall short of completion due to the high volume of signals generated by network monitoring. Pushing these signals into a SIEM is economically expensive, requires analysis to be created which relies on individual knowledge, and can also overwhelm enterprise SOC teams with too many alerts. Data-centric security solutions should avoid reliance on a SIEM by capturing the full context of all the pathways to the data and natively performing analytics. These solutions would then only send the results of the analytics to a SIEM. This allows necessary insights to be centrally gathered without the cost of processing the raw signal data or relying on individual knowledge to correctly generate analysis.

## 4. *Activity requires context*

Context is key to disrupting an attack chain, and visibility is required from the edge of the application or website to the database in order to get it. The context needs to be gathered at each stage of a pathway as well as in aggregate. The complexity and dynamic nature of modern environments necessitates this context for efficient investigations of incidents by SOC teams. Furthermore, data-centric security solutions need to ensure they don't overwhelm SOC teams with alerts by performing analytics prior to sending results and insights to a SIEM.

## **CONCLUSION**

As data-centric views in environments continue to become common, a strong data-centric security strategy will be key for the success of enterprises. Data continues to be gathered in large volumes from ever increasing sources which requires a strong security strategy that starts at the data-layer to help enterprises ensure there is no leakage of sensitive information and facilitate data access.



An aerial photograph of ocean waves crashing onto a sandy beach. The water is a vibrant turquoise color, and the foam is white and frothy. The sand is a warm, golden-brown color. The text "DISTINGUISHED VENDORS" is overlaid in white, bold, uppercase letters in the upper right quadrant.

**DISTINGUISHED  
VENDORS**



## DISTINGUISHED VENDORS

Q 3 2 0 2 1

**W**orking 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 and 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.

### 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.

### anjuna

Cloud adoption continues but concerns over secure usage remain. The confidential cloud provided by Anjuna facilitates the move to secure cloud by leveraging the hardware-grade secure enclaves available by the major cloud providers.

Anjuna's confidential cloud helps secure all applications, databases, AI platforms, and custom and packaged code.



Avanade was founded as a joint venture between Microsoft and Accenture. 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.

# TAG CYBER DISTINGUISHED VENDORS

2 Q 2 0 2 1



Balbix was founded to help companies 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.



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.



Email is one of humans' most-used tools – for work and even for personal business. Yet, many email-focused security solutions aren't sufficient to stop the prevalence of attacks that start with email. Egress provides human-layer, intelligent email security to stop phishing attacks and business email compromise.



With its acquisition of Signal Sciences, Fastly is vying to become the world's leading edge security provider, offering secure content delivery API security, and a cutting-edge web application firewall. The company's mission is to provide real-time visibility and protection via cloud-native solutions.



DNS data offers insights into attacker domains and infrastructure. But many enterprises don't leverage DNS because traditional tools are too noisy and complicated. HYAS offers a next-gen protective DNS (PDNS) platform that helps security teams reduce the attack surface by identifying and blocking known maliciousness.

# TAG CYBER DISTINGUISHED VENDORS

2 Q 2 0 2 1



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.



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 to reimagine the perimeter.



OpenText™ Security Suite, powered by OpenText™ EnCase™ — industry-leading cyber forensics technology — provides 360° visibility into data-centric threats across endpoints and servers. With a long history in enterprise information management, OpenText offers forensic-grade security solutions which help security teams make faster decisions and rapidly remediate threats.



Prevaillon reduces companies' mean time to detect and mean time to respond. Prevaillon's Compromise Intelligence™ tool, beacons out and collects data on attacker TTPs as well as target victims. Unprecedented insight into attacker networks gives security teams the ability to identify and prevent cyber compromise.



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.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 1



The Randori platform was designed to think and act like the attacker groups executing ransomware attacks. The platform identifies attack targets and illuminates where and how attackers will strike. Randori allows enterprises to find vulnerabilities, prioritize remediation, and close points of entry before they're exploited.



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.



The Sertainty data privacy platform protects organizations from data compromise by embedding intelligence and protection directly into data. Built on a self-governance model, Sertainty allows security, operations, and DevOps teams to create policies that dictate how data can be accessed and by whom.



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.



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.



Shift5 protects operational technology from cyber compromise. Led by former military cyber experts, the company allows critical infrastructure companies to operate without significant cyber risk. Through data capture, visualization, analytics, and alerts, the Shift5 platform helps operators find and detect events and prevent cyber incidents.



# TAG CYBER DISTINGUISHED VENDORS

2 0 2 1



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' individual business requirements.



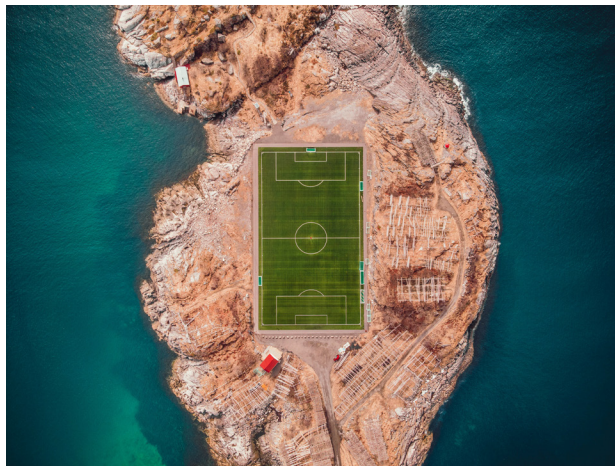
Application protection is imperative for organizations of all sizes. Virsec provides runtime workload protection at all layers. With full visibility into workloads and a patented mapping technology, companies can get a handle on what's running in their environments and prevent known and unknown bad from executing.



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.



To truly drive down cyber security risk, enterprises must focus on threat-centric security operations. ThreatQ by ThreatQuotient improves security operations teams' workflows, delivering analytics and an automated, orchestrated management plane for threat intelligence management, threat hunting, incident response, vulnerability management, and more.





**TAG**CYBER

© 2021