

TAG Cyber

Security Annual

3RD QUARTER 2022



CHINA & CYBERSECURITY

A S P E C I A L
S E C T I O N

ARTICLES / OPINIONS / INTERVIEWS

WELCOME TO THE 2022 TAG CYBER SECURITY ANNUAL 3RD QUARTER EDITION



LESTER GOODMAN,
DIRECTOR OF CONTENT,
TAG CYBER

**Opinions. Viewpoints. Articles.
Perspectives. Research. Interviews.
And observations. Truly original observations.**

At TAG Cyber, we do not shy away from controversy. You'll find a healthy dollop of controversy in this edition. You'll probably encounter an article in here that you like. And you might also find something that you hate. It's that sort of report.

Our focus here is on China. Specifically, *cybersecurity* in the context of the People's Republic of China. Where other industry analyst firms refuse to go, perhaps to protect their revenue—well, we go there. Not having obscene wealth in the coffers does have *some* advantages. Here we say what we think.

That's what we've got for you in this 3rd Quarter Edition of the 2022 TAG Cyber Security Annual: China and Cybersecurity.

From Dr. Jennifer Bayuk's well-researched compendium to Chris Wilder's tough warnings about Chinese global actions, and David Hechler's incisive article sharing Paul Rosenzweig's expertise, you will find here many different well-reasoned views on the current cyber challenges from China being faced by Americans and others.

Dr. Edward Amoroso makes the claim that the U.S. global supply chain policy toward Chinese firms such as Huawei and ZTE is useless. You won't want to miss this. Ed's article and the others in this volume are complemented by interviews with iconic leaders from the security industry.

The core cybersecurity issue regarding China, of course—one that everyone agrees with—is that all nation-states have become too good at cyberoffense. This includes the United States, the United Kingdom, Russia and many other countries. They've all become too good at breaking into systems. Much too good.

China, of course, is one of the best when it comes to cybersecurity—particularly on offense. But an unanswered conundrum is why they've been so relatively quiet in security start-ups. Name, for example, a Chinese security start-up you've used in the past three years.

For this reason and others, we are all now forced to address geopolitical issues that have never been part of the purview of the IT security specialist. It's caused cyber experts to download global maps to look up countries and regions that might affect or influence their work.

As always, we hope that you will benefit from our research. We thank our Research as a Service (RaaS) customers in enterprise and our Content as a Service (CaaS) customers in the security vendor community for providing the support to enable our research and writing. It is through their kind support that we can offer this volume to readers for free.

We hope you find it useful.

Lester Goodman, Director of Content

David Hechler, Editor

Contributors

Ed Amoroso
Jennifer Bayuk
David Hechler
Jessica Andrus Lindstrom
John Masserini
Gary McAlum
Christopher R. Wilder

Editorial & Creative

Lester Goodman
David Hechler
Michelle Perino
Julius Washington
Judy Lopatin
Miles McDonald
Rich Powell

Research & Development

Matt Amoroso
Shawn Hopkins

Sales & Customer Relations

Rick Friedel
Trish Vatis
Laurie Mushinsky

Marketing

Scott Krady
Tony Taddei
Leona Laurie

Administration

Liam Baglivo
Julia Almazova

Ed Amoroso, Founder & CEO



Volume 8 No. 3

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871
Copyright © 2022 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 2022 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, 2022

C O N T E N T S

Introduction	2	Detecting Threats and Reducing Supply Chain Risk Using ReversingLabs Mario Vuksan, ReversingLabs	56
CHINA & CYBERSECURITY	5	How Enterprise Teams Can Achieve Identity Security Using SailPoint Mike Kiser, SailPoint	59
Why U.S. Restrictions on Chinese Software Will Have No Impact on Cyber Risk	6	Implementing Cloud Data Fragmentation for Enterprises Using ShardSecure Bob Lam, ShardSecure	62
How China’s World Colonization Plan Impacts Cyber	9	How Sicura Supports Compliance Across IT, Operations and DevOps Lisa Umberger, Sicura	64
Chinese Attacks on U.S. Technology: A View from the Trenches	12	Comprehensive Cloud Protection Using Sonrai Security Eric Kedrosky, Sonrai Security	67
Balancing Security in Business with China	20	Protecting Executives from Cyberthreats with Sunday Security Tsachi Ganot, Sunday Security	70
LEGAL	24	A New Approach to Data Protection from Titaniam Arti Raman, Titaniam	73
What’s the Role of the U.N.? Where’s the Line on Neutrality?	25	ANALYST REPORTS	76
You Need a Network to Defeat a Network	31	Introducing Cloud Data Fragmentation (CDF)	77
Fighting Even Over Definitions of Fighting	37	Next-Generation Vulnerability Assessment and Patch Management: An Overview of Acronis Cyber Protect Cloud	84
INTERVIEWS	38	Automating Cybersecurity Posture Assessment: An Overview of the Balbix Platform	89
An Intelligence-Driven Approach to XDR from Anomali Mark Alba, Anomali	39	Real-Time Mitigation of Cyberthreats to APIs: An Overview of the Salt Security Platform	95
Concierge Digital Protection for Corporate Executives and High-Access Employees from BlackCloak Dr. Chris Pierson, BlackCloak	42	Making the Case for Digital Identity Protection as an Enterprise Control	100
Using Cymulate to Optimize Security Posture Dave Klein, Cymulate	45	DISTINGUISHED VENDORS	104
Identifying Threats in Network Traffic Using Cynamics Dr. Aviv Yehezkel, Cynamics	48		
Securing Cloud Data Using Laminar Amit Shaked, Laminar	51		
Managing Third-Party Cyber Risk Using Prevalent Brad Hibbert, Prevalent	53		

A S P E C I A L S E C T I O N

CHINA & CYBERSECURITY

WHY U.S. RESTRICTIONS ON CHINESE SOFTWARE WILL HAVE NO IMPACT ON CYBER RISK

DR. EDWARD AMOROSO

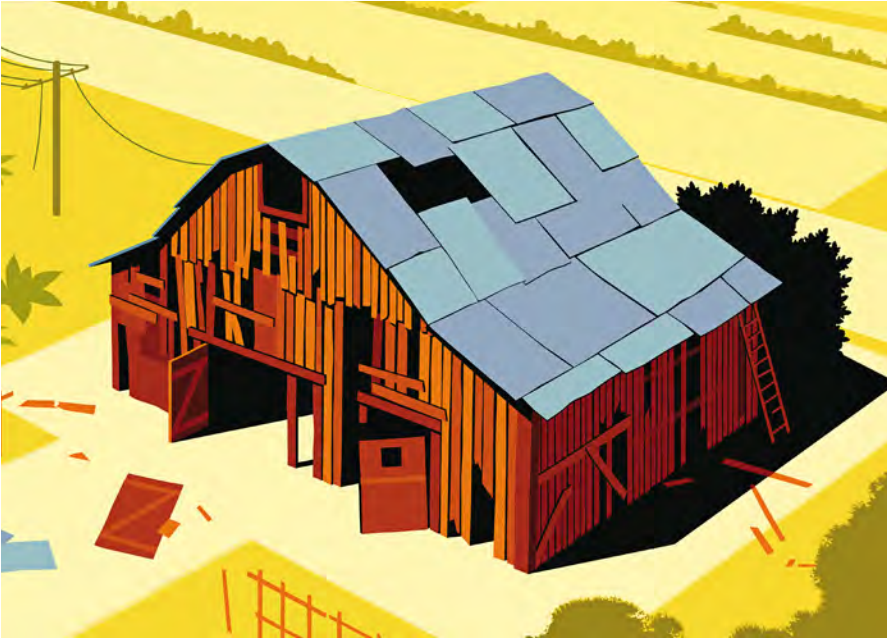


The actual cybersecurity benefit of Chinese product avoidance is nearly zero.

Here's something that every Washington lawmaker believes: Products from companies such as Huawei and ZTE are rigged with Trojans inserted under the direction of the Chinese government. They believe further that such malware could be invoked remotely to steal valuable intellectual property and interrupt essential services in the United States.

Viewed from this perspective, policy restrictions on the purchase of Chinese products would seem both sensible and necessary. And we know from Ken Thompson's seminal Turing address, based on his work at Bell Labs, that Trojan insertion is easy. One might thus be led to conclude that avoidance of Chinese products would have a material impact on cyber risk.

Unfortunately, the actual cybersecurity benefit of Chinese product avoidance is nearly zero. Furthermore, focusing our collective energy on this aspect of the



If you were to point to cracks in the roof as a primary issue, any reasonable observer would have to question the risk prioritization.

cyber risk equation diverts valuable time and attention from the real problem: our severe and nagging vulnerability in the United States against conventional cyberbreaches.

Let's start with the mistaken belief that Chinese government coercion can only work for companies headquartered in China. It's as if we think that malware could only be inserted into a product with full management cooperation. The view conjures the image of some conspiratorial meeting between company executives and the government to approve the Trojan plan.

In reality, government coercion would never be done this way. The approach instead would involve pressuring an individual with the right access and skills. This targeted entity would have a background or situation that could be used as influence leverage. And their supervisor would have no knowledge of the scheme. There would be no need to share this information.

This is a key observation, because such coercion could be done at virtually *any major technology company*. This includes Google, Microsoft and any other vendor with team members connected to China. Let me repeat: Avoiding software from companies headquartered in China does not remove the risk of Trojans in our software being controlled by China.

Now let's examine the mistaken belief that a nation-state needs Trojans to steal intellectual property or to disrupt systems. This is a patently absurd notion. Every cybersecurity expert knows that U.S. assets are regularly stolen or degraded by nation-state actors using basic offensive measures such as phishing, lateral traversal and DDOS.

An analogy might help: Imagine an old barn with broken doors, windows missing and cracks in the sidewalls. Obviously, if someone wanted to enter your barn, they would just come in through the open access. If you were to point to cracks in the roof as a primary issue, any reasonable observer would have to question the risk prioritization.

And never mind the view that it might be more obvious and dangerous to come in through the open doors—perhaps because of increased surveillance or security. The analogy does not hold for cyber:

Malicious nation-states have been coming in through our open gateways and access for many years. There has been zero need to leverage risky Trojans to steal data.

Finally, let's review the unfortunate consequence of focusing our supply chain security on country-specific avoidance. When we do this, we introduce the mistaken impression that we've reduced cyber risk in a material manner. And this can have a disastrous impact on control priorities and security budget by diverting attention away from meaningful security issues.

If policymakers decide to avoid China or any other country for reasons related to politics, economics or other noncyber matters, they should be clear about their motivation. But by pinning the issue on the cybersecurity community, they dilute public understanding of the real decision drivers, and, as explained above, they introduce harm to our nation's cyberposture.

The only reasonable cybersecurity policy for the United States is to significantly bolster our defenses. The details of this are beyond the scope of this article, but the main aspects of the approach would involve reduced complexity, increased resilience and greater focus on addressing our skills gap in security and information technology.





HOW CHINA'S WORLD COLONIZATION PLAN IMPACTS CYBER

CHRISTOPHER WILDER

Telecommunications infrastructure, especially the internet, is a massive challenge and opportunity in Africa and the Middle East (MENA). While each has an enormous population, it has limited access to the internet. The governments across MENA and other developing countries struggle to bring connectivity to their people. The increased demand for connectivity has created openings for foreign telecom providers, especially from China, to step in and offer their predatory lending, expertise and technology providers, like China's own Huawei, ZTE and others.

CONNECTIVITY AND SECURITY AT A COST

China's belt and road initiative (BRI) is the country's strategy to invest in critical infrastructure projects worldwide. For the past decade, China has partnered with over 140 countries to build ports and highways; improve rail; and upgrade power stations, airports and communications infrastructure, with predatory lending and repayment schemes that bankrupted its unwitting victims. Further, China's BRI initiative has constructed most of the major undersea internet cables critical for MENA's connections to the internet and the world. Undersea internet cables represent most fiber optic cables worldwide. They are responsible for ferrying nearly all internet traffic in and out of the countries, creating significant cybersecurity and data harvesting challenges for China's

“partner countries,” which account for almost 70% of MENA’s 4G internet infrastructure. China’s 4G global dominance gives the nation a substantial advantage. With the developed world transitioning to 5G, it is unrealistic for these countries to change incumbent providers midstream. China is effectively setting up data and intelligence listening posts for the countries they claim to help. State-funded hacker and cracker organizations are diligently working to support China’s BRI ambitions. For example, China currently has over 40 hacker organizations working to breach and exploit government operations (46 attacks in the last three months), financial services (27), industrial (17), telecom (15), and energy and utilities (14) worldwide.



Source: 2022, TAG Cyber/TruKno

Huawei, ZTE and other Chinese companies are deeply coupled with the People’s Liberation Army and are subject to China’s National Intelligence Laws. Specifically, Article 7 states, “Any organization or citizen shall support, assist and cooperate with the state intelligence work following the law, and keep the secrets of the national intelligence work known to the public.” These companies collect intelligence, monitor users/detractors, and steal secrets and intellectual property to help China’s army further its questionable goals, regardless of borders. There is no doubt that China’s cheap networking and communications equipment collects data and intelligence, monitors detractors and steals intellectual property via known cybersecurity weaknesses and backdoors.

Further, over the past six months, we at TAG have identified 20 Chinese-based bad-actor organizations, deploying nearly 70 newly organized and targeted cyberattack campaigns in BRI countries and beyond. These groups include Bronze Starlight (RAT and ransomware), TA428 (malware, downloader, backdoor), Aogin Dragon (backdoor, APT), Flubot (bot attacks), etc. In June 2022, researchers discovered that the hacker group Aogin Dragon had operated espionage/spying/listening and APT activities since 2013, targeting government, education and telecommunications organizations throughout MENA and Australia—without detection.

THE DEVIL IS IN THE DETAILS— BE CAREFUL WHAT YOU WISH FOR

For developing countries, China's BRI is a "Faustian bargain" to bring MENA into the next generation of its internet infrastructure. China's tactics allow it to cement its presence as the primary provider of internet and critical infrastructure in MENA. On its current pathway, China will corner Africa's markets for future iterations of the internet while enhancing its intelligence-gathering capabilities. MENA sees the promise of increased connectivity and modernization, but it comes at the cost of privacy and freedom. Western governments must provide viable alternatives to Chinese aggression and ensure a future where the free world doesn't have Chinese spies, hackers and observers looking over its shoulders.

China's BRI is a "Faustian bargain" to bring MENA into the next generation of its internet infrastructure.



China's BRI program, on the surface, is attractive for politicians and bureaucrats to improve their infrastructure, create new jobs and remain in power. However, China's efforts come at a high cost for these countries. For example, China partnered with the former president of Sri Lanka to deploy several megaprojects, including a new deep-sea port, airport, roadways and a new convention center. The government eagerly entered a financial agreement that caused Sri Lanka to sink into an unsustainable debt situation. Per the deal's terms, China seized the deep-sea port. Several politicians, including the soon-to-be former president of Sri Lanka, are facing indictments and long jail sentences. Recently, Cambodia agreed to build a new deepwater port. When the government defaulted on the agreement, China evicted its tenants and established a large Chinese Navy base in its place, thereby establishing a major security threat in the region.

A CALL TO ACTION

Most governments and organizations have failed to adequately respond to China's colonization efforts. We believe that it is a good start to have the Group of Seven (G7) pledge to inject \$600 billion in private and public funds to develop and enhance the needed infrastructure to counter China's multitrillion-dollar investment in BRI projects. The role of Western governments and telecom providers must invest in similar initiatives and projects and deliver a viable alternative to China's networking and communications equipment. Sadly, the response may be far too little, too late.

CHINESE ATTACKS ON U.S. TECHNOLOGY: A VIEW FROM THE TRENCHES

JENNIFER BAYUK

The U.S.-China Economic and Security Review Commission (USCC), founded in 2001, wrote in its first annual report that China's goal was to quickly close the gap between the United States and its own capabilities in technology warfare.¹ A key element of China's strategy was to exploit U.S. complacency and outwit the U.S. with "Sha Shou Jian"—assassin's mace weapons. These are literally clubs, but figuratively are methods to balance asymmetric power by "using cheap things to undo expensive ones."² A Chinese president in the 1980s was frequently quoted as pushing an internal policy to "hide your capabilities and bide your time" and to "absolutely not take the lead in world affairs."³ This came as no surprise to U.S. diplomats because of an ominous dictum, oft-repeated in diplomatic circles dating back to the 19th century:⁴



**China is a sleeping giant, let her sleep
for when she wakes, she will shake the world.**

In the years since China went public with "Sha Shou Jian" and even earlier, U.S. actions to safeguard cyberspace—or more to the point, inaction—have played into China's hands. Rather than fortifying our infrastructure about China's cyberattacks, the U.S. government preferred to rely on 19th century diplomacy. Rather than admit that critical infrastructure was inherently vulnerable, U.S. companies preferred to downplay the negative impact of repeated blows from the assassin's mace. Most of us working in cybersecurity could only look on in horror. Those of us who did make a big public fuss were dismissed as "Chicken Littles."⁵ Here is a historical perspective from our trenches.

2000–2005

Since 2002, the U.S. Department of Homeland Security (DHS) has coordinated efforts to share information on cybersecurity threats to U.S. critical infrastructure with the infrastructure owners via a National Infrastructure Protection Plan (NIPP). It recruited industry regulators to convene CISOs to join forces in Information Sharing and Analysis Centers (ISACs) for each critical infrastructure industry. Through the U.S. Secret Service, DHS shares classified threat information with these ISACs, and also shares publicly available government research on cyberthreats. Also in 2002, the U.S. Federal Bureau of Investigation (FBI) established a Cyber Division, which a year later was assigned program responsibility for InfraGard, an information sharing and analysis program previously established in field offices to foster public-private trust/credibility in the exchange of information concerning terrorism, intelligence, criminal and security matters.

Coincident with these initiatives was the establishment of the USCC. Created by Congress in October 2000, its mandate was to monitor, investigate and report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, for government action.

Those of us working in critical infrastructure cybersecurity became keenly aware of the extent to which our companies had become targets of nation-state information warfare. At the beginning, cyberattacks⁶ seemed very targeted. For example, there was competitor espionage, revenge by disgruntled employees and credit card scams.⁷ The latter made the financial industry a prime target, so the Financial Services ISAC ("FS-ISAC") was under heavy pressure from regulators to protect the American consumer. The number of records in data breaches was being reported in the tens of thousands and that seemed shocking at the time. It was enough to create awareness in business and opinion sections of newspapers, but rarely on page 1. It took destructive worms that disabled infrastructure for anyone other than techies to notice that "computer security" was a trending issue.

Nevertheless, cyberdefenders became a necessary part of critical infrastructure, and we developed fast response and recovery strategies. I personally went "to the mattress" by throwing my gym matt on the floor next to my landline speaker phone, monitoring and coaching a plethora of desktop support people around the globe as they cordoned off networks and patched PCs. The U.S. government was too busy building offensive capabilities to do anything more than warn us. We were hosted at lavish conferences and dinners by cybersecurity vendors who were getting paid to deliver zero day threats (security bugs in our vendor's code!) to nation-states (including our own).⁸

Throughout this time, the USCC published a steady stream of information on China's disregard for World Trade Organization rules on theft of intellectual property⁹.

The transfer of technology by U.S. investors in China as a direct or indirect government-imposed condition of doing business with Chinese partners remains an enduring U.S. security concern as well as a violation of China's WTO agreement. A WTO complaint should be filed when instances occur.



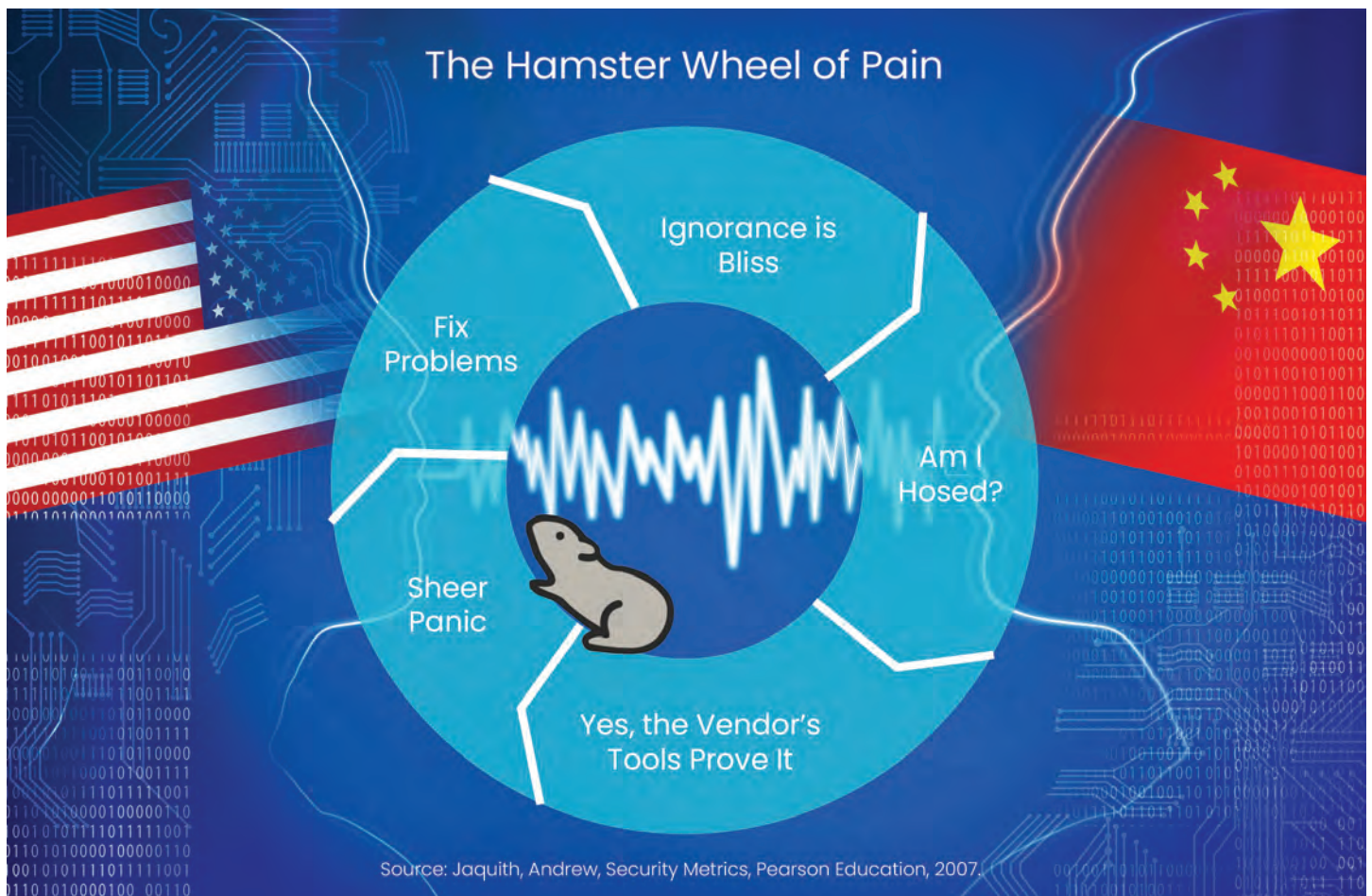
What China does with its growing technology capabilities—whether it converts them to military uses and/or to control the free flow of information to its population—is of direct national security concern to the United States.

Internally, we were identifying and responding to an endless stream of new cyberattacks, and threat actors were typically cloaked in anonymous internet traffic. Now that we know it was Chinese strategy to be entering this field, we can safely attribute some percentage of that activity at that time to China (as our adversaries, also with good basis in probability, attribute similar activities to the U.S.). Why didn't we lobby for more government involvement in defense? A significant issue was that few CISOs had permission to admit their systems had not been resilient enough to withstand the attacks. This caused considerable debate within the FS-ISAC. One CISO would ask another: "What impact did SQL Slammer have on your systems?" The other would yawn and say they were shopping for lawn furniture over the weekend, what did they miss? Yet we all knew we had our own version of mattresses.

At least in the financial industry, I understood this mindset. I saw examples in the 1990s. New York Stock Exchange computers would go down for hours, but it was never picked up by the financial industry press. No Wall Street firm wanted to risk public panic at the idea that the newfangled technology would not be able to keep track of their money, so no one in the whole industry complained in any way that might hit the papers. The mindset was that these computer security events, like unplanned outages, would also pass.

2006-2009:

One industry analyst mockingly called our predicament cybersecurity's "hamster wheel of pain."¹⁰ A wheel of pain is a reference to ancient and medieval servility where slaves labor on turnstiles or prisoners are attached to torture mechanisms. The caged hamster (CISO), however, voluntarily embarks on the spinning wheel and continues to run as the wheel turns faster instead of trying to get off. The joke was that we were treating cyberattacks as sets of remediation projects without recognizing and remediating the root cause; that is, intent adversaries persistently hunting for vulnerable systems. Though we worked harder and faster, we never got ahead.¹¹



As time went on, our participation in industry ISAC and InfraGard events provided us with ample evidence that China was unabashedly committing espionage on the U.S. government and businesses, as well as political opponents and dissidents. One of the more fascinating trails of events was China's infiltration into NASA.¹² Consequences of these attacks included a satellite diverted off course, supercomputers being physically unplugged from the network, and theft of data on rocket engine design, space shuttle operations and financial planning. Such activity was linked to network addresses in Taiwan and China. Yet there was no viable remediation activity. Rather, there is evidence that NASA officials instead retaliated against those who reported the events. Like Wall Street, NASA did not want to shake faith in its mission, so it played down both current and potential future negative impact. This response was unfortunately the norm rather than the exception. To understand the impact of this complacency among the victims requires acknowledging that it advanced China's strategy, which was specifically designed to foster such complacency. China played on our inherent aversion to bad news in order to fly under the political radar.

Mid-decade, the U.S. military adopted the term "Advanced Persistent Threat" (APT) to give a name to China's type of unrelenting targeted espionage. One of China's People's Liberation Army (PLA) Units has the dubious distinction of being the first such labeled cyber threat actor: APT1.¹³ Its detectable activities have been tracked back to 2006, but it was likely formed earlier (NASA's attacks are known to date back to 1998). The ISACs continued to evolve into more structured information-sharing capabilities, providing anonymous or severely restricted distribution levels to allow cyberattack details to reach other potential victims. Though not as prominent, the USCC continued to feed us observations, and in 2007 added "key recommendations" with a strong focus on cybersecurity. In 2007 and 2008, the USCC recommended that Congress should:¹⁴

ensure adequate support for protecting critical American computer networks and data: The Commission recommends that Congress assess the adequacy of and, if needed, provide additional funding for military, intelligence, and homeland security programs that monitor and protect critical American computer networks and sensitive information, specifically those tasked with protecting networks from damage caused by cyber attacks.

APT had become a well-known term in cybersecurity, but the practical implications of the term "APT" had not risen to the attention of business leaders. The temptation of China's great untapped marketplace was irresistible, and despite the fact that cybersecurity APT was high on the operational risk lists, U.S. business leaders accepted those risks and dove into China's marketplace.

Early in 2008, I was part of a committee sent to Washington by my Wall Street employer to testify before the U.S. Committee on Foreign Investment in the United States (CFIUS).¹⁵ The topic was a joint venture with a Chinese securities firm wherein we would provide back office services to support operations related to financial transactions. My role was to persuade the committee that we would be entirely in control of all the software used to process the transactions, that the Chinese members of the Joint Venture population would have no administrative or software development capability, and that our networks would ensure that all of our firm's intellectual property remained within U.S. borders. I did my best. Luckily for me, the financial crisis made the case moot. It remains for me a striking example of the differences between perceptions of threat in government and industry. Government was becoming more agitated while industry preferred to remain naively optimistic.

Though each industry ISAC member understood that risk of being a victim was increasing, the hamster wheel was in frenzied rotation and most felt they were at least one step ahead of the bad guys. Only those with cross-industry global views more fully understood the bigger picture.¹⁶ In March 2009, TAG's own Ed Amoroso joined a group of distinguished cybersecurity experts who testified to the U.S. Senate that revenues from cybercrime exceeded those of drug crime, and were worth some \$1 trillion annually. To those who understood the full extent of China's intellectual property theft, this figure was well within the range of plausible. To others in the trenches, however, it seemed like an unproven hypothetical. "What are they thinking?" sighed some CISOs, especially the less experienced ones. "They are crying Chicken Little, and we'll all be dismissed as overreacting." After all, at the time the latest USCC report had no recommendations on cybersecurity. When their companies plunged headfirst into China's marketplace, they were all-in.

By 2009 the tone of the USCC recommendations had changed. Rather than recommend that Congress spend on protection for all critical infrastructure, it recommended only that funding be provided to government to "meet the rising challenge of Chinese human intelligence and illicit technology collection," to "respond" to attacks, and to "develop effective and reliable attribution Techniques" for attacks. Where U.S. companies were mentioned, it was to recommend that Congress make sure they were not helping China (or other authoritarian countries) with censorship.¹⁷ By the end of the decade, we knew not just from DHS and FBI, but also from increasingly credible news reports and observations of our own systems, that theft of intellectual property, denial of service attacks and malicious surveillance from China were steadily increasing. Nevertheless, none of USCC's 2007-2008 recommended protection assistance was forthcoming.

2010-2014:

The situation aligned perfectly with Sha Shou Jian. Yet the 2010 report had no substantive guidance other than that Congress request the administration to report on such hacking activity.¹⁸

The Commission recommends that Congress request that the administration periodically issue a single report about the volume and seriousness of exploitations and attacks targeting the information systems of all federal agencies that handle sensitive information related to diplomatic, intelligence, military, and economic issues.

I thought it ironic that Congress had created a standing committee of experts to give them advice on this topic, and their advice was to ask someone else for a report.

One of the companies that was profoundly impacted by the pending government initiatives to deter internet censorship was Google. Yet to all appearances, its joint venture with China was successful. Like FS and NASA, the tech giant also had a tendency to hide from news of its vulnerability.¹⁹ Circa December 2009, Google's cybersecurity staff started to detect anomalous activity on internal networks that had no explanation other than deep-rooted occupation by a data-thieving APT.²⁰ Within a month Google had evidence that its network was overrun with Chinese espionage agents who had infiltrated hundreds of machines with the aim of gaining access to both gmail accounts and source code. Many of us in the trenches heard rumors that, in a brash effort to eject the APT, Google trashed all of its Microsoft PCs

and made staff switch to Apple Macintosh.²¹ We applauded, though not sure whether to believe it. Soon after the public statements started to emerge, Google closed its Chinese internet search service and rerouted its search traffic to its uncensored service in Hong Kong.²²

Further investigation soon revealed that dozens of U.S. tech companies had been similarly treated by China.²³ USCC alarm bells with respect to cybersecurity were back.²⁴

The penetration of Google's computer network this year has renewed concerns about the Chinese government's tolerance or possible sponsorship of malicious computer activity.

USCC reports in 2011-2014 more regularly highlighted specific attacks, including but not limited to: RSA's networks breached by "Honker Union of China" hacker group,²⁵ a history of the NASA attacks, including full functional control over networks,²⁶ and successful large-scale espionage against DoD, DoD contractors²⁷ and the US Postal Service.²⁸ The outcry from U.S. business became too much for the U.S. government to ignore, and for the first time ever criminal charges were filed against known state actors for hacking. Five PLA members were indicted.²⁹ From the trenches, this was widely viewed as "security theatre," or as some referred to it, "keeping your friends out," because the only people who would bother to abide by your rules are your friends; your enemies are easily able to ignore them. The five indicted PLA members never apprehended.

As the diplomats applauded the indictments, China was given a breather from focus because other nation-states were more visibly throwing their weight around in cyberspace. North Korea decimated Sony Pictures, Iran launched denial-of-service attacks against U.S. banks, Russia took down the internet and power grids in Estonia and Ukraine. These attacks seemed more alarming than China's unobtrusive though steady siphoning of U.S. secrets.

2015-NOW

Though China may have receded from the foreground in 2013-2014, a book published in 2015 brought a stark reminder that the China's intention to see Sha Shou Jian achieve objectives was a highly plausible threat.³⁰ Ghost Fleet portrays a scenario in which China starts a war against the United States using cyberweapons as its primary attack vehicle. The authors "spent years gathering information on everything from the next generation of Chinese drones to the ways in which certain U.S. weapons systems have already been hacked.... information is ... tucked into announcements of government contracts ... U.S. and Chinese military reports, online forums, and even leaked photos on Chinese social-media sites of ships under construction."³¹

If that did not persuade all of us hamsters of the reality of the threat, for the rest it hit home when we received official letters from the Office of Personnel Management that our own personal data has been compromised.³² Though we did not work for the federal government, it was a condition of our participation in the DHS-run ISACs that all industry participants must have secret clearances. The online forms we filled out to apply for the secret clearances included the most detailed personal information we had ever been requested to provide: job history, past residences, travel outside the U.S., all of our family members and their birthdates. More than enough information needed to answer security questions if you were unfreezing a credit report or logging into the IRS. Our own government could not secure its own top secret clearance systems. It could not protect its cyberdefenders.

In 2016, USCC acknowledged that no actions taken by the US or anyone else in the past 15 years of its operation has deterred China to deviate from its Sha Shou Jian strategy for world domination:³³

China continues to violate the spirit and the letter of its international obligations by pursuing import substitution policies, imposing forced technology transfers, engaging in cyber-enabled theft of intellectual property, and obstructing the free flow of information and commerce.

Nevertheless, recent history shows improvement only on the individual indictment side, not in the more ominous systemic threat. The U.S. government's ability to detect and identify accountability for APT cybercrimes improved to include apprehension and prosecution of culprits. The 2019 USCC reported Department of Justice prosecutions of individuals associated with China's cyberattacks, including but not limited to:³⁴ October 2018—an alleged deputy division director in the Jiangsu Department of China's Ministry of State Security, for recruiting aerospace employees from companies like GE Aviation to divulge trade secrets; Oct 2018—10 individuals, including members of Jiangsu Department of China's Ministry of State Security, for conspiring to steal sensitive data related to jetliner turbofan engines; December 2018—APT10 members, working in association with China's Ministry of State Security's Tianjin State Security Bureau, for economic espionage targeting U.S. government agencies and private companies across a broad array of industries for over a decade; April 2019—a Chinese businessman and U.S. engineer, for stealing turbine engine technology from GE Power.

Nonetheless, against the backdrop of persistent Sha Shou Jian, the prosecutions seem like more security theatre. Especially so, given that our current FBI director recently declared:³⁵

China's reached a new level—more brazen, more damaging than ever before.

The U.S. belief in conventions such as the rule of law, mutually agreed goals of business joint ventures, and diplomatic resolutions to intellectual property rights violations have not made a dent in the persistent advance of China's progress toward its goal of global supremacy. The U.S. government's belief that these conventions would halt or even slow China's steady progress built on systematic theft and repurposing of U.S. data and intellectual property now seems naive and utterly ineffectual.

All indications are that China's strategy of "hide your capabilities and bide your time" has now given way to "shake the world." Ironically, NASA administrator Bill Nelson seems to be the first to emerge from slumber, recently saying:³⁶ "We must be very concerned that China is landing on the moon and saying: 'It's ours now and you stay out.'" Let us hope this creates a groundswell of concern leading to an appropriate defense, which in this case is most certainly not just a good offense.



Footnotes

¹ Pursuant to Public Law 106-398, October 30, 2000 as amended.

² Hambling, David, "China Looks to Undermine U.S. Power, With 'Assassin's Mace,'" *Wired*, July 2, 2009, <https://www.wired.com/2009/07/china-looks-to-undermine-us-power-with-assassins-mace/>

³ See full explanation of the quote at: <https://history.stackexchange.com/questions/54862/what-does-deng-xiaoping-mean-by-hide-your-capacities-bide-your-time>

⁴ See Fish, Issac Stone, "Crouching Tiger, Sleeping Giant," *Foreign Policy*, 1/19/16, https://foreignpolicy.com/2016/01/19/china_shakes_the_world_cliche/ Also note that "giant" is sometimes written as "lion" or "dragon," depending on the source

⁵ This is a reference to a children's story where a chicken thinks the sky is falling because an acorn fell on its head.

⁶ Which, if you research, you should know at the time cyberattacks were referred to as "computer security attacks" or "information security breaches" or simply "hacking" or "viruses."

⁷ See for example, NYT Times Archives on searchwords like "information security," "computer virus" and "computer security," <https://www.nytimes.com/search?dropmab=true&endDate=20041231&query=computer%20security&sort=best&startDate=20020101>

⁸ Perloth, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*, Bloomsbury, 2021.

⁹ USCC 2004 Annual Report, p. 24 and 12.

¹⁰ Source: Jaquith, Andrew, *Security Metrics*, Pearson Education, 2007.

¹¹ Even before Jaquith's analogy, we in the trenches referred to the situation less specifically as "Whac-A-Mole," an analogy with a still-popular 1970s game where the goal is to strike mechanical/virtual rodents with a mallet as they incessantly pop up in scattered patterns from numerous holes.

¹² Summarized from Epstein, Keith, and Ben Elgin, "The Taking of NASA's Secrets," *Business Week*, December 1, 2008, pp 73-79.

¹³ Mandiant, "APT1 Exposing One of China's Cyber Espionage Units," <https://www.mandiant.com/media/9941/download>

¹⁴ USCC 2007 Annual Report, p.16. The 2008 wording is very similar, USCC 2008 Annual Report, p. 18.

¹⁵ CFIUS evolved from Defense Production Act of 1950 and a 1988 amendment, Section 721 of the legislation was revised by the Foreign Investment and National Security Act of 2007 (FINSA), establishing CFIUS authority to review foreign investments in U.S. business and real estate.

¹⁶ Senate Commerce Committee, Hearing on Improving Cybersecurity, Statement of Edward Amoroso, <https://www.commerce.senate.gov/services/files/EBD018C6-BF5F-4EA6-9ECC-A990C4B954C4>, March 19, 2009. <https://www.itnews.com.au/news/cyber-crime-profits-running-into-trillions-of-dollars-141172>

¹⁷ USCC 2008 Annual Report, p. 14.

¹⁸ USCC 2011 Annual Report

¹⁹ Perloth, *This is How They Tell Me the World Ends*, 2021, ch. 5

²⁰ *Ibid*, ch 14

²¹ *Ibid*, includes mention of an overnight raid wherein Google removed Microsoft PCs from staff offices without warning

²² Helft and Barboza, *Google Shuts China Site in Dispute Over Censorship*, *New York Times*, March 22, 2010, <https://www.nytimes.com/2010/03/23/technology/23google.html>

²³ *Operation Aurora*

²⁴ USCC 2011 Annual Report

²⁵ USCC 2011 Annual Report

²⁶ USCC 2012 Annual Report

²⁷ USCC 2013 Annual Report

²⁸ USCC 2014 Annual Report

²⁹ US Department of Justice, Office of Public Affairs, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>

³⁰ Singer and Cole, *Ghost Fleet: A Novel of the Next World War*, 2015.

³¹ See *Ghost Fleet's* authors' description of their research in: "How to Write About World War III," *The Atlantic*, 6/30/15, <https://www.theatlantic.com/international/archive/2015/06/ghost-fleet-world-war-iii/397301/>

³² Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People*, *Washington Post*, July 9, 2015, <https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>

³³ USCC 2016 Annual Report

³⁴ USCC 2019 Annual Report

³⁵ Wray, "Countering Threats Posed by the Chinese Government Inside the U.S.," *Federal Bureau of Investigation*, <https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122>

³⁶ Glenn, "NASA chief warns against China's moon program," *The Washington Times*, July 5, 2022.

BALANCING SECURITY IN BUSINESS WITH CHINA

DAVID HECHLER

Like a lot of China-watchers, Paul Rosenzweig has serious concerns about the country's role in the world of technology. Take TikTok. He knows there are pointed questions about how well ByteDance, the Chinese company that owns it, protects user data. That was the issue that recently led Federal Communications Commissioner Brendan Carr to urge Apple and Google **to ban TikTok** from their app stores. And that's also an area in which Rosenzweig has a special interest. But he's even more concerned about another matter: TikTok's sway over public opinion. "It's a vehicle for the exercise of influence in the same way Facebook is, but it's one that is not responsive to American values, or in the end, American control," he said. "And that's a danger."



Paul Rosenzweig

TikTok could spread false information after an American election. And then what? "We don't prohibit speech," Rosenzweig said, "because we're too afraid of the adverse results—and by the way, that's the right answer. But that means that we really don't have a way of censoring TikTok, when and if it is used to create a false impression about the election." And we've seen enough of that to appreciate the potential scope of the problem. "It's easy to identify the problem," he added. "It's very hard to see the solution."

Paul Rosenzweig is a lawyer who pays a lot of attention to China. It's not because he's had a longstanding interest in the country. It's about business. He's devoted his career to subjects that make China impossible to ignore: national security, privacy and cybersecurity. His legal work often extends well beyond representing clients in legal disputes. He seems drawn to big issues that raise public policy debates.

Recently he led **a study** conducted by the **Lawfare Institute** on what makes tech products and services trustworthy. The executive summary didn't get past the second paragraph before China made an appearance. There was one case study in the 52-page report. It involved the sale of a U.S. company to, you guessed it: a Chinese firm. He told me about the project when I was planning our interview. He only mentioned it once when we talked two days later, but it seemed to underpin a lot of our conversation.

It's not as if Chinese companies are all extensions of their government, Rosenzweig said. Many of them, like [Alibaba](#), have some degree of independence. But at least in the technology sphere, they are "handmaidens," he said. "That independence is severely constrained in ways that are unfamiliar to Western, capitalist impulses," he added.

Alibaba was an apt example. Founder [Jack Ma](#) was the country's ultimate capitalist success story—until he criticized the country's regulators and banks a couple of years ago, which resulted in a swift response from China's leaders. They scuttled the scheduled IPO of the Ant Group, Alibaba's affiliated financial arm, and opened an antitrust investigation that caused the company's stock price to crash. As Rosenzweig noted, Alibaba's "freedom was more illusory than real. And when they strayed too far from the party line, they were reeled back in."

Rosenzweig brings an unusual perspective to the challenges in this field. He went to law school at the University of Chicago, which immerses students in the doctrine of law and economics, which proved to be a good grounding for what followed. His interest in public policy and national security were given a big boost when he was the deputy assistant secretary for policy in the early days of the U. S. Department of Homeland Security. He went on to found Red Branch Consulting, which specializes in homeland security and data privacy. And he began teaching a course at George Washington University in cybersecurity law and policy in 2010. He believes it was one of the earliest offerings on the subject in the country. And he's still at it.

APPLE V. HUAWEI

The day before we spoke, FBI director Christopher Wray and MI5 director general Ken McCallum held an unprecedented [joint press conference](#) in London to talk about economic and national security risks their two nations face from China. Wray warned that American businesses don't recognize the threats



MI5 Director General Ken McCallum (left) and FBI Director Christopher Wray at a joint press conference at MI5 headquarters, in central London.

There was one case study that was quite different. It was about accusations that our government had behaved badly—to professionals in the United States who had once lived in China.



to their independence that come from being too deeply engaged with China. The Chinese government, he said, is "set on stealing your technology, whatever it is that makes your industry tick, and using it to undercut your business and dominate your market."

I asked Rosenzweig how the U.S. government should respond to the threat that China represents. "The best U.S. policies are appropriately contextualized," he said. This requires "a legitimate risk assessment," he went on. "What's the threat? What's your vulnerability? What are the consequences?" Some products are no threat. Buying a pencil manufactured in North Korea doesn't require a policy.

"If it's a company like Huawei asking to put its servers into our 5G network, you probably want to do a serious risk assessment," he said. "And more likely than not, the result is that you want to shy away from that altogether, and buy your gear from Ericsson out of Sweden."

The U.K. actually went so far as to test Huawei's suitability for 5G. The Brits established the Huawei Cyber Security Evaluation Center and required **multiple rounds of tests**. Competing companies were exempt. Rosenzweig and many others viewed this approach as a mistake. Others were harsher, deeming the entire exercise political theater. "I think they realized that no degree of testing is, by itself, sufficiently adequate to guarantee the trusted nature of a particular piece of gear," he said. "You have to evaluate the corporate structure, and then the superstructure of the national laws and policies within which the corporation operates." It's not easy to evaluate the trustworthiness of Huawei or, say, Apple equipment, he acknowledged. And many have given up hope. "I'm unwilling to be despair-ridden at this point," he continued. Sounding like the man who has long sought to **measure cybersecurity**, and who seems convinced there's a way to quantify confidence in Apple v. confidence in Huawei, he added: "I think we should try."

"No degree of testing is, by itself, sufficiently adequate to guarantee the trusted nature of a particular piece of gear. You have to evaluate the corporate structure, and then the superstructure of the national laws and policies within which the corporation operates."

USER DATA IS NOT ALL THE SAME

There's a reason Rosenzweig is not as concerned about the privacy of personal information as others who complain about TikTok are. The explanation is found in three letters: OPM. In 2015, China stole 22 million records in the **U.S. Office of Personnel Management data breach**. It was one of the largest government breaches in U.S. history, and Rosenzweig's classified data was in there. "If you fill out one of those forms," he recalled. "you basically bare your soul. If you're doing it honestly, and I did. And so China has everything that they could possibly want to know about me. And liking a particular TikTok video, or resharing it, or whatever it is you do on TikTok, wouldn't change that very much."

He did allow, however, that all data is not the same. In the Lawfare Institute trustworthiness project, the case study that involved China featured the sale of the gay dating app Grindr to a Chinese tech company. The sale was reviewed by the Committee on Foreign Investment in the United States (CFIUS), which routinely reviews sales of sensitive U.S. companies for national security risks. In this case, CFIUS forced the Chinese buyer to sell Grindr back to a U.S. company, and the sensitivity of the personal information was a prime reason. "Grindr data, the OPM breach—those are much different than these kind of open source Facebooky things," Rosenzweig said. "You want to set your privacy levels so only your friends see your drunken bacchanal on the rooftop," he added. "But at the same time, it's just a drunken bacchanal on the rooftop. It's not being in the closet in a country that stones homosexuals to death."

There was one unofficial case study that I brought up as our conversation wound down. This one was quite different, though it also involved trust. It was about accusations that *our* government had behaved badly—to professionals in the United States who had once lived in China. I thought it was worth taking a look in the mirror.

THE CHINA INITIATIVE

Rosenzweig's background seemed perfectly suited to address this matter. He'd begun his legal career as a trial lawyer at the U.S. Department of Justice. He'd later served as investigations counsel at the U.S. House of Representatives. Later still, he was a member of the D.C. Bar Legal Ethics Committee. And, of course, he's been teaching cybersecurity for a dozen years.

In 2018, under President Trump's first attorney general, Jeff Sessions, the Justice Department began investigating professors and researchers who were working at U.S. colleges and universities. Under what it called the **China Initiative**, the FBI opened literally thousands of investigations in an effort to end what was thought to be massive spying and theft by academics of Chinese origin. They were accused of being secretly loyal to China.

Indictments were brought against dozens of teachers. One was **Gang Chen**, a professor of mechanical engineering at MIT and a U.S. citizen. He was arrested in January 2021 for failing to disclose his ties to China in an Energy Department grant application. A year later, according to CBS News, the Energy Department told prosecutors that they'd gotten it wrong. Soon after the charges were dismissed. But the damage had been done.

By late February 2022, there had been so many acquittals and dropped charges that the department was widely and loudly accused of bias. After an internal review, DOJ said that it was ending the China Initiative. A DOJ official denied any suggestion of racial bias, but acknowledged that the initiative had been "myopic" and may have created the appearance of prejudice.

Rosenzweig was troubled. "I find myself deeply conflicted by this particular problem. On the one hand," he said, "it is abundantly clear that China is attempting to use money and influence to shape the academic debates in America. They've funded **Confucius Institutes** in a number of universities, many of which are closing now as people recognize the dangers. So China clearly sees the American academic scene as one that it can influence. On the other hand," he continued, "it's utterly anathema to me to target an individual on the basis of their ethnicity, or on the basis of their politics, or on the basis of what they're working on."

There is no equivalency here to what happens in China. The accused were able to defend themselves and prevail. The criticism came from all over, including from Rafael Reif, the president of MIT, who quickly decided that Prof. Gang Chen had done nothing wrong and that the school would pay his legal fees. Reif also spoke publicly against the China Initiative. And eventually the Justice Department backed down. These things don't happen in China.

Reif agreed that China has stolen intellectual property from the United States. "We do have a problem with China," he told CBS News. "We are not playing by the same rules. All I'm saying is, just going to universities and looking for Chinese Americans and doubting their loyalty to this nation is not the right approach."

Rosenzweig led a group that wrote about trust in hardware and software, and he talked about corporate culture, and the national laws and policies that surround it. But ultimately, trust is up to humans. Reif told CBS that the prosecutions were "scaring the best talent in the world, which we need in this country, from coming into this country." And Gang Chen sounded like a man whose trust had been permanently broken. "I am no longer the Gang Chen I was before," he said. "From my family, the trauma we experience, the fear we still have, to my professional career. My research group is gone. I will no longer be the same person."



LEGAL

WHAT'S THE ROLE OF THE U.N.? WHERE'S THE LINE ON NEUTRALITY?

RUSSIA'S INVASION OF UKRAINE HAS RAISED INTERNATIONAL LEGAL QUESTIONS LIKELY TO PROVOKE DISCUSSION FOR YEARS.

AN INTERVIEW WITH ERIC JENSEN

Shortly after Russia invaded Ukraine on February 24, we **interviewed** Brigham Young University law professor Eric Jensen about the cyberwar that was in its earliest stages. Professor Jensen is an expert on the law of armed conflict and national security law. There was a lot to talk about—too much to include in one article. For example, we'd asked this expert on the United Nations whether any international organizations were in a position to change the war's course. Later, we asked him to comment on developments that followed our earlier conversation, including war crime trials in Ukraine. We also asked if the countries supporting Ukraine have crossed the neutrality line. That's an aspect of the conflict that he predicted "will be one of the things that most profoundly affects international law in the next couple of decades."

TAG Cyber: We want to ask you some questions about the United Nations. The Security Council was asked to **take action against Russia** for its invasion of Ukraine, but Russia has a permanent seat on the Security Council. Is there anything the U.N. can do about a war in which one of the parties has veto power over any resolution?

ERIC JENSEN: Well, unfortunately the U.N. doesn't have—or maybe fortunately, I don't know; it depends whose view you take. But the U.N. does not have a methodology to demand recusal from a permanent member of the Security Council on an issue in which they have an interest. And, of course, that's been important to the United States over time as well. The United States has been very happy **to not have to recuse itself** from activities where it was engaged in military operations. So I think that the Security Council is functioning as it was designed to function. You could certainly envision a scenario where the General Assembly, through something called the **Uniting for Peace resolution**, could wrest control of those international security issues where a member of the Security Council was involved. But that's not how the current U.N. structure was designed to function.



The United Nations Security Council Chamber

TAG Cyber: *We did note that in March the U.N.'s International Court of Justice ordered Russia to withdraw its troops. First, did this surprise you? And second, did anyone imagine that it would have any effect?*

JENSEN: Yeah, great question. The International Court of Justice is in a bit of an odd spot with respect to this. It's not like the Supreme Court of nations around the world, where when the parties come before the court, they have an obligation to do what the court says. The International Court of Justice is a court of consent. There are two ways you can consent to its jurisdiction. One is "I'm always going to be part of its jurisdiction." And the other is "I'm going to only participate in the cases that I'm interested in." And both the U.S. and Russia take the latter view. And so Russia never appeared before the court for those hearings, as they wouldn't. It was a one-sided argument. Everybody already knew how that was going to turn out because everybody who knows international law already knows that Russia has been in violation of international law since **Crimea in 2014**, not just since the most recent invasion. And so there was no doubt that the court was going to come out against Russia. And, as you implied, no doubt that Russia was going to ignore whatever the court said. But as a matter of law, of course, the court is right.

Though Russia was able to veto a Security Council resolution demanding it stop its invasion and withdraw its troops, other countries, including the United States, have been happy to veto resolutions aimed at them.

TAG Cyber: *Is there any entity that has the power and the wherewithal to enforce norms or understandings or even treaties designed to protect international peace?*

JENSEN: Well, aside from the 15-nations Security Council, which under Article 24 and Article 25 can demand nations do what they say, I think that what we're seeing in the world today is exactly what is the alternative, which is nations merging together by consensus and using tools, like sanctions and other things, to put significant pressure on a recalcitrant state. Now, there's always the resort to force, right? I mean, all of these same nations that are joined together on economic sanctions could also then resort to force and evict Russia from Ukraine. But I think that that would just widen the war and, of course, cause lots more casualties. And hopefully, if this works, we can—it's obviously horrible what's happening in Ukraine—but it would be worse if it was happening in Ukraine, and Poland, and Moldova, and Germany, and the United States and everywhere else.

TAG Cyber: *So it seems, if you're hoping for some sort of action by a court to enforce international laws against crime of this sort, it's really only ex post facto that periodically, every few years, maybe every decade, some leader is hauled to the Hague to face criminal charges—often years after the war in question. Is that as far as the U.N. and international courts go?*

JENSEN: You're hitting on two really important issues there. The first is the International Court of Justice, which is really a forum where states can argue and get resolution. And it's not just Russia that has ignored the ICJ. China has ignored the ICJ with respect to the South China Sea. The United States, in a very **famous case in 1984**, ignored the ICJ with respect to what was going on in Central and South America. So that is not unusual, unfortunately. Now, your point about hauling some leader of a nation to court. Of course, that person would not appear before the International Court of Justice. He or she would appear before the International Criminal Court, as you said, and yes, that is in retrospect. But the hope is that the deterrent value of punishing a leader who does a crime of aggression, which might be the case here, would convince other leaders to not do that in the future. So not only would you get

In May 2022, Russian soldier Vadim Shishimarin pleaded guilty in a Kyiv courtroom and was convicted of killing a Ukrainian civilian. He was sentenced to life in prison in the first war crime trial since Russia's invasion in February.



Maxym Marusenko/NurPhoto via Getty Images

retribution on that individual leader, but it would also hopefully act as a deterrent on future leaders. Now there's a lot of study on that. And it's really a matter of question whether there is a deterrent value to prosecuting leaders. I think it's inconclusive.

TAG Cyber: *And those trials, they often go on for years.*

JENSEN: Yeah. And a huge expense, right? I mean, \$25 million is a pretty good number of what it costs to get one conviction at those international tribunals. You can make an argument that there might be better ways to use that money.

TAG Cyber: *During our first conversation, you spoke of the possibility that Russian soldiers might be prosecuted locally for war crimes. Since then, we've learned of instances where that's happened. What laws apply, and could Russia try to turn the tables?*

JENSEN: In the United States, we have a War Crimes Act that allows us to prosecute people who commit war crimes, either U.S. persons or persons who commit war crimes against U.S. persons. A similar domestic law should exist in countries across the world who are signatories to the Geneva Convention. Which Ukraine, of course, is. And so they would use their domestic law to prosecute Russian soldiers for violations of international law or the law of armed conflict.

TAG Cyber: *And if Russia decides that crimes have been committed against its soldiers by Ukrainian forces, is there anything that would prevent them from taking action similar to what we've already seen the Ukrainians do?*

JENSEN: No, that should be the exact same rule. In fact, as you mentioned, Ukraine's prosecuted several Russian soldiers already for their actions on the battlefield—**one pretty notorious one** that's come to full fruition. Notorious not in a bad way, notorious in that it's happened and a lot of people are talking about it. And the Russians should legally be able to do the same thing to Ukrainians. Though, of course, the big one that's hitting the news now is not the Russians prosecuting Ukrainians, but the **Russians prosecuting those two British men**. And the reason this is different is because when you prosecute the soldiers of the nation you're fighting, it's pretty clear what law applies. You prosecute them in accordance with international law and the law of armed conflict. They get immunity for their warlike acts that are in compliance with the law. They should be treated as prisoners of war. All that seems pretty clear. With these two British soldiers, it's a little different because they aren't members of the Ukrainian military. Now, that doesn't mean they're not covered by the law of armed conflict. But what the Russians have said—and we don't really know enough facts to be able to answer this question—is that these two

are mercenaries, and therefore they will be tried under domestic law, and they've sentenced them to death. Now, it's pretty clear that they're probably not mercenaries. So Russia is probably wrong in classifying them as mercenaries. International law is pretty clear on what it takes to be a mercenary. One of the key points that is unlikely to have been met in this case is you have to have been recruited by the promise of large sums of money. And that has to be your incentive—to get the money—and you have to have been given the money. And it seems pretty unlikely that that's the situation of these two British citizens. Most likely they're just activists who are supporting Ukraine in the fight against Russia. Now, would they meet the definition of people who are protected as prisoners of war? Also probably not, unless they were somehow working in conjunction with the Ukrainian military and had been incorporated into those forces. So, they're probably just going to be tried under common criminal law.

TAG Cyber: How might the Geneva Conventions be invoked as this particular war continues?

JENSEN: One of the interesting aspects of this, and we hit on this a little bit in our prior conversation, is that the Geneva Conventions provide universal jurisdiction for war crimes. Not simple breaches of the law of armed conflict, but for grave breaches there's universal jurisdiction. So if a Ukrainian soldier who is alleged to have committed a war crime, or a Russian soldier who is alleged to have committed a war crime, shows up in any country in the world, if that country has implemented that provision of the Geneva Conventions, they could be tried in those countries as people who have committed grave breaches of the Geneva Conventions.

TAG Cyber: And what's the definition of "a grave breach"?

JENSEN: Each of the four 1949 Geneva Conventions contains a list of grave breaches that is supplemented by the 1977 [Protocol I and Protocol II](#). It's things like experimentation on prisoners of war, or killing prisoners of war or killing civilians. They're certainly the kinds of things that have been alleged by both sides in this conflict.

TAG Cyber: The United States, Poland and the United Kingdom have all contributed lots of weapons to Ukraine's war effort. And yet, they are not considered to be at war. They are neutral parties and want to remain neutral parties. What would they have to do to cross the line that separates a neutral state from a state engaged in war?

JENSEN: This is a really interesting aspect of this conflict that I think will be one of the things that most profoundly affects international law in the next couple of decades. There is a convention from 1907 called The Hague Conventions. And [Convention V](#) deals with neutrality and land warfare. And Articles 7, 8 and 9—what they say is that there's no prohibition in Article 7 of supplying weapons to countries in armed conflict. That doesn't violate neutrality in and of itself. Article 8 says it's OK to help with communications and allow communications across your country. That doesn't take away your neutrality. But what Article 9 says is, in the applications of Articles 7 and 8, if you're going to do things like supply weapons or allow communications, you have to do it equally and you have to allow it to both countries. Now, this is where I think countries like the U.S., and Poland and the U.K. are in trouble. Because we're not selling weapons to Russia. In fact, we're sanctioning people who are engaged in that kind of business with Russia. So the U.S. has taken this neutrality and adapted it and created a

Under the Geneva Conventions, individuals accused of grave breaches of the law of armed conflict can be tried in any country to which they travel that has implemented that provision of the Conventions.

term—“benevolent neutrality”—which basically means we’re going to be nice to the countries involved in armed conflict that we want to, and not be nice to the countries we don’t want to. So we’re going to facilitate Ukraine by selling arms, we’re not going to facilitate Russia by selling arms. This is, I think, technically in violation of Article 9 of the Hague rules. But the U.S. took this view even during World War II, so it’s a longstanding view. Under the U.S. view, what they would have to do to cross the line, as your question intimates, is they would have to actually participate in the war. Not just supply weapons, but maybe supply people. We’re already supplying intelligence to them, right? We’re not supplying intelligence to Russia, but we are to Ukraine. So under a technical reading of Hague V, we’ve probably already crossed that line. But if we actually now started sending forces to Ukraine, that would be a violation even of the U.S.’s view of this benevolent neutrality.

TAG Cyber: *What about sending over people to train the Ukrainian forces, especially in using some of the high tech weapons we’ve supplied that they have no experience using? That’s providing personnel not to actually fight, but to advise.*

JENSEN: One of the weapons systems that we have potentially sent or are contemplating sending is the MLRS, the multiple launch rocket system. We would have to send not only the weapons system, but some kind of technical advisers to ensure they knew how to properly use it. The supply of advisers to use those weapons systems probably does not cross that line under the U.S. view.

TAG Cyber: *Some of the high tech weapons that we know countries like to use these days are drones. They can be operated from a great distance, as we have done for years. Isn’t it tricky to know who’s actually controlling the drones? I mean, if we had our personnel, our advisers in Ukraine, or maybe in Poland, they could be directing the weapons, not just talking about them. They could also be directing weapons like drones from an even more remote location. Would that cross a line?*

JENSEN: Let’s make a differentiation between drones that gather intelligence and drones that might launch ordnance. We’ve been supplying satellite imagery and other intelligence to Ukraine. Under the technical view, that might be a violation. Under the U.S. view, probably not. But let’s transition now to say it’s not just unmanned or unarmed drones, now it’s armed drones, it’s a Predator or some other type of drone that can actually launch munitions. Let’s assume that, like many of the drones the U.S. uses worldwide, it’s operated out of Creech Air Force Base in Nevada. That, it seems to me, clearly crosses the line, because now you have a U.S. person in the U.S. operating a weapon system that’s used against Russia, in Ukraine. What if instead of being operated out of the U.S., it’s operated out of Poland or even Ukraine itself? If it’s a U.S. person operating in Poland, or in Ukraine, and he is actually flying the drone and pushing the button, again, I think you’ve crossed the line. Even under the U.S. view. If it is a Ukrainian person who is operating the drone, and the U.S. person is just standing behind them and saying, “Yes, you’re steering it right. Yes, the guidance system is working well. Yes, that’s the button that you need to push, when you push it.” I don’t think that crosses the line under the U.S. view. The hardest one is if the person standing behind the Ukrainian soldier is saying, “OK, press the button now.” You’re right at the line. And for mem, that crosses the line.

TAG Cyber: *With robotics advancing as ineluctably and swiftly as they are, there will probably come a time when, instead of sending what we’re sending, we’ll send robots that can actually operate the equipment, and then we’ll have a whole different problem.*

JENSEN: Or just send autonomous weapon systems that all you have to do is push start, and then they do it all themselves, right? You know cybertools are in this same category. And we know that China conducted some cyberattacks against—I use that word “attack” hesitantly. Let me say China conducted some cyberoperations against Ukraine, in the build-up to Russia’s invasion in February. But they weren’t of a nature that would cross that line to make China also a combatant in the current conflict. The U.S. has clearly been assisting Ukraine, as has the U.K. in their cyberprotective measures, and potentially

even cyberoffensive measures against Russia. It's the same kind of question, right? I mean, when the cybertool is created, and all it takes to initiate it is the pushing of the enter button on your keyboard, does the creator of the cybertool somehow become implicated? Or is that just like selling a weapon system where you don't cross that line? Emerging technologies definitely make that a harder discussion.

TAG Cyber: *Does that mean there are going have to be modifications to the Geneva Conventions? Technology is changing the laws all over the place. It's always in advance of the law. You're one of the guys who would be answering this kind of question. So, is that where we are now? Do we need some people trying to figure out new rules, and new conventions and new treaties?*

JENSEN: You're right, this is exactly the kind of stuff I spend my time thinking about, working on and talking with governments about. But I don't think we need new rules. We need to think clearly about how the rules apply to new technologies. We've had this same problem many times in our history. Think back to the use of balloons at the turn of the 19th century. And then you think about submarines in the 1920s. And you think about aircraft, the way we started using aircraft in the early 1900s. All of these were new technologies that people said, "How are we going to respond to this when it's applied in armed conflict?" And nations figured out ways to do it. And we've used the same rules. We've sometimes had to adopt or adapt on the fringes, and adopt new ways of looking at it, but it hasn't caused wholesale change in the law of war. I think we're in the same position now. Things like cybertools, virology, autonomous weapon systems, robotics, nanotechnology—all of these emerging technologies that are on the cusp of being developed, that will most certainly be weaponized. I don't think it's going to make us reinvent the law of armed conflict. But we are going to have to be very thoughtful in how we apply the existing rules to those new technologies.





YOU NEED A NETWORK TO DEFEAT A NETWORK

M Y
T A K E

DAVID HECHLER

WHEN A GERMAN INVESTIGATOR AND PROSECUTOR WERE TAPPED TO TACKLE CYBERCRIME, THEY DIDN'T KNOW THEY'D BE WRESTLING A GIANT BOTNET.

When I've written about the importance of alliances in cybersecurity, most often I've focused on collaborations between the public and private sectors. But Russia's invasion of Ukraine has spotlighted the need for countries to work effectively together. And that reminded me of a long interview I did in 2021 in which Ukraine figured prominently. So did Russia, but the subject was not the conflicts between them. It was the international cooperation required to bring down a botnet.

It was a Zoom conversation with an investigator and a prosecutor from Germany. They had worked together for four years on this project, and they won an award for leading a coalition that took down the notorious network known as **Avalanche**. In doing so, they managed to secure the help of dozens of countries. I knew that Ukraine was one of them, but I'd also read something shortly before our conversation that had surprised me. Russia and China had also helped the cause. I was eager to ask about that.

There were other reasons this story seemed important. Even though cybersecurity was not a household word in 2009, when the botnet was first identified, the criminals who used Avalanche were a far cry from earlier generations of hackers. They were often sophisticated operators who specialized in certain tasks, like planting malware, crafting phishing emails and laundering the cash they stole. When they joined together, they didn't even know each other's names. Many only knew their confederates by their handles, which afforded them a layer of protection.

And most of them operated with virtual impunity from Eastern Europe. The companies they victimized were nearly all in Western Europe and North America. The gangs were careful not to target companies in countries



Frank Lange



Jörn Bisping

like Russia, from which quite a few of them operated. As long as they didn't steal from Russians, they seemed to be able to count on that government's indifference to their activities—and very few of the other countries they frequented had extradition treaties with Western nations.

These threats have not vanished since the demise of Avalanche. They've only expanded in recent years. Botnets come and go, but they are not going away. Nation-state cyberattacks are still the most feared. And some criminal gangs that specialize in ransomware, for example, are not only operating under the tacit protection of nations, sometimes their members are also working for those countries.

All of this underscores the importance of nations banding together to defend against attacks—and to attack the sources of the threats. That's why there's much to be learned from the takedown of a giant.

THE BIG ONE

Jörn (pronounced Yawrn) Bisping and Frank Lange (Languh) had each spent years pursuing organized crime. Bisping as a police officer in Luneburg, in the Lower Saxony region of Germany. Lange as a senior prosecutor in Verden, also in Lower Saxony. When we spoke, both were in their home offices as a result of the Covid pandemic, and I noticed a small poster on the wall next to Lange's bookshelf. At one point, Bisping was explaining the ways in which their experience in organized crime gave them a leg up when they moved to cyber. The organized crime cases were categorized as high level, he said, and they required working with counterparts in other countries.

"Frank," I said, "is that why you have a picture of Marlon Brando in *The Godfather* on the wall behind you?"

Lange smiled. "He's the one I want to get," he shot back. "It's my target."

In 2009, Brando and *The Godfather* were certainly well known, but cybercrime was just starting to attract widespread attention. It wasn't until 2012 that the German police organized a specialized unit of 10 officers that Bisping was tapped to lead, and Lange was put in charge of two prosecutors who concentrated on cyber. Their partnership started with the investigation of 200 ransomware attacks (which were far from commonplace back then).

"Do you remember, Frank?" Bisping began. In Germany, unlike the United States, prosecutors work closely with police investigators from the very beginning. They actually sign a contract. When they began investigating what turned out to be Avalanche, they were searching for a way to stop the attacks. But they had no idea what they were embarking on. It was as though they'd decided to do a little fishing—the old kind of fishing, off a bridge on the Rhine—only to discover that they'd hooked the Loch Ness Monster.

The first thing that became clear was that Germans weren't the only victims of the cyberattacks they were uncovering. As they started digging, what they were seeing was multidimensional. It took a long time before it came into focus. There were victims in a number of countries. And the perpetrators were not a single gang running a scam. There were several running different "campaigns," as Lange called them. And it wasn't easy to separate victims by location. "It's not possible to cut one piece out of it only to get the German part," Lange said. It made more sense to go after the whole enterprise.

It was as though they'd decided to do a little fishing—the old kind of fishing, off a bridge on the Rhine—only to discover that they'd hooked the Loch Ness Monster.

The way to do that was to work with law enforcement in the other countries under attack. So they gathered information about as many victims as they could, and then looked for partners to collaborate with.

MEETINGS

It took time. If you want help from law enforcement in other countries on a big project, you aren't likely to make headway by sending a letter, Bisping and Lange explained. "Because if you take the official way and send a letter and ask for something," Lange said, "maybe you get an answer a few weeks later, a few months later, a few years later." The better way, he continued, is to "ask if you can go there and talk with them."

This "personal contact" changed everything. After they shared the information they had, their counterparts had skin in the game. They had their own victims and "their own interest in getting ahead with this case," Lange said. And they saw value in joining this international law enforcement network. Each had the opportunity to pitch a story to their local media, "and so everyone had his benefit from this."

Bisping agreed, but added that it took a lot of work. The easiest partnerships were with their counterparts in the European Union. The Germans had high praise for **Europol** and **Eurojust**, both headquartered in The Hague. If they wanted to meet with officers in an EU country, all they had to do was call Europol and someone would make the arrangements. But that didn't mean it was always easy to establish trust, Bisping emphasized.

Some countries were running parallel investigations. Sometimes it took lots of meetings to establish rapport. There were clashes of philosophies and processes when they began working with Eastern European countries like Georgia and Ukraine, Bisping noted. "What will happen when we give them the data?" he wondered when they began talking to investigators in Ukraine. "It's a big question, but especially in the field of cyber." In the end, he said, "a lot of countries recognized that it is the best option we have to work together. Perhaps the only."

The challenge was getting all of the countries on the same page. "Because all of the countries are organized differently," Bisping said. It was more of an issue for prosecutors than police officers, he added, but it affected both. It took time to work through these differences. And as they did, they began to recognize the strengths and weaknesses of their respective systems, and how they could blend these to benefit their work.

For example, U.S. companies store a lot of data. So U.S. investigators have access to vast historical databases, Bisping said. But not the Germans. Europe has much stricter privacy laws, and there are no large databases to check. But they do have large central internet nodes through which most of the traffic passes. And this was particularly useful because Eastern Europeans, including the Avalanche perpetrators, were reliant on Western European internet infrastructure. "So out of this," Bisping said, "we were able to get real-time data from our side for the investigations—better than the U.S. guys could, because they have to do legal requests to get data from Europe."

As they gathered victims' data out of the botnet infrastructure, they could bring what they'd found to law enforcement in the different countries. "You have the following problem," Bisping would say, and then he'd show them. It was a surefire way to get their attention—and draw them in.

This proved pivotal. As they gathered victims' data out of the botnet infrastructure, they could bring what they'd found to law enforcement in the different countries. "You have the following problem," Bisping would say, and then he'd show them. It was a surefire way to get their attention—and draw them in.

There were benefits law enforcement derived from the wave of attacks. As cybercrime was expanding, so was the European response. In addition to countries' creating specialized units for police and prosecutors, in January 2013 Europol launched its **European Cybercrime Centre** (known as EC3) to help EU states dismantle and disrupt these crime networks. Bisping and Lange may have been among the early responders, but like it or not the world was discovering cybercrime, and international botnets that spread the pain were also spreading the word.

BULLETPROOF HOSTING

But even with new-found partners, it took years of investigating. Why?

What they were pursuing was complicated. **Botnets** may comprise a network of dozens, or hundreds or thousands of infected computers that criminals command and control. And unbeknownst to the owners of these internet-connected devices, gangs use them to advance and conceal their crimes.

Avalanche was a particularly sophisticated network because it used a fast-flux system that featured numerous IP addresses associated with a single domain name, and these were rapidly swapped to evade detection. So it wasn't easy to follow the criminals' trail. Lange and Bisping spent a lot of time requesting search warrants, searching for servers and, once they found them, examining and wiretapping them. And they had to coordinate these activities in almost every country in Europe.

But that wasn't all. It wasn't just ransomware they were up against. As they dug deeper, they found one strain of malware, and then another and another. They worked with professionals from the Fraunhofer Institute who reverse-engineered what they'd found. "We developed a lot of skills," Bisping said of his team, "but we needed these experts." They were able to identify about 20 types of malware, he noted, that were deployed by a number of different gangs.

So when they were chasing Avalanche, it wasn't just a gang, or a type of malware or a botnet they were up against. It turned out to be a service—a so-called **bulletproof hosting** service run by an administrator who allowed a variety of gangs to use the infrastructure. He also provided gangs with money laundering services and their pick of malware.

The administrator was their target, and taking down the entire infrastructure was their goal. But before they began the arduous and uncertain process of trying to destroy it, the Germans and their counterparts in the United States were determined to find and arrest the administrator. And the best way to do that, they agreed, was to go after one of the gangs that used his services.

That was how a federal prosecutor from the Western District of Pennsylvania, and an investigator from the FBI's Pittsburgh field office, came to pursue the GozNym (pronounced GoesNeem) malware gang, which I wrote about [here](#) and [here](#). The gang had victimized many companies in Pennsylvania. Of the 11 members investigators connected to the crimes, five were based in Russia and deemed beyond the grasp of Western law enforcement. But one was located in Bulgaria, which had an extradition treaty with the United States. He was eventually shipped to Pittsburgh, where he pleaded guilty. And two others were located in Georgia, where they were ultimately tried and convicted.

Avalanche's alleged administrator was traced to Ukraine. He, too, was arrested, though it's unclear how long he was confined, and he doesn't seem to have faced charges related to Avalanche. (When the police came knocking, he shot at them through his door and he was arrested for that.) What surprised many observers on both sides of the Atlantic, including those who worked in law enforcement, was that

Georgia and Ukraine had agreed to work with U.S. and Western European lawyers and police officers in the first place. And that Georgia had agreed to prosecute a case that was built on evidence that involved victims outside its borders.

To Bisping and Lange, these were the fruits of four years' labor. They happened because, in response to an international crime wave, people in far-flung places who were sworn to keep the peace were willing to meet—and then work together.

SINKHOLING

November 30, 2016, stands out as a red-letter day. That was when Gennady Kapkanov, the alleged Avalanche administrator, was arrested in Poltava, Ukraine. But that wasn't the most important event that day for Bisping and Lange. It was also the day Avalanche died.

At the time, Bisping said, the bulletproof hosting network was "one of the biggest of the world. Perhaps the biggest." He estimated that it had hosted an average of 20 malware campaigns and maybe 60–70 different ones over the years. Eradicating the operation required cooperation on a different scale than the arrests and prosecutions.



It wasn't the first big takedown of a giant botnet. [Gameover Zeus](#) preceded it. And there were lots of lessons they'd learned from that one. It had been run by Evgeniy Bogachev from Russia, and it took a huge international effort, and more than one try, to knock it out. Operations like Gameover Zeus don't rely on a single botnet, Bisping explained. "They have fallback systems," he said. "So if one campaign or some botnet goes down, the good ones"—the skilled administrators—"have fallback areas they can switch to."

Lange agreed. "The Gameover Zeus takedown was a model for us," he said. "You have to take down the whole infrastructure from where this botnet runs, and you have to coordinate all over the world." He added: "We learn from it how to sinkhole. We have seen how it is possible to sinkhole a botnet."

Sinkholing in this context redirects traffic from infected computers to servers controlled by law enforcement. That was the biggest challenge. According to the [Europol press release](#), 37 on-site searches were conducted, 39 servers were seized (another 221 were knocked offline through abuse notifications sent to the hosting providers), and 800,000 domains were either seized, blocked or sinkholed. "The operation marks the largest-ever use of sinkholing to combat botnet infrastructures," the release said.

Victims of malware hosted by Avalanche were found in 180 countries. It took the concerted efforts of investigators and prosecutors in 30 countries to bring it down. And here again, nations used methods that played to their strengths. The Germans did not have civil laws they could use in sinkholing, but the United States did and used these extensively, Lange said. U.S. law enforcement was also able to partner with companies like Microsoft (which German government officials could not do). And like the investigators who finally sank Gameover Zeus, Bisping, Lange and their partners were constantly looking over their shoulders, wondering whether Avalanche would be resurrected. More than 10 months after it was downed, Bisping addressed the issue in a video: "A lot of people said, 'OK, how long it might work, days or weeks now?' And this is what we are lucky about. It worked until today. Avalanche is still down."

BANDING TOGETHER

The video was created by the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) after it named Bisping and Lange winners of the **2017 JD Faulk Award**. The international membership organization, based in San Francisco, honored the duo “for spearheading worldwide efforts to dismantle the criminalized Avalanche platform.” In the [video](#), the two men were characteristically generous with their praise, naming individuals and organizations that helped the effort. “We had, of course, some countries who didn’t want to be named,” Bisping noted. That didn’t surprise me. But I was surprised by two countries he did name: “There was unprecedented cooperation worldwide, including registries in Russia and China taking down malicious domains....”

My understanding is that Russian cybercriminals can usually rely on some level of protection if they’re in Russia and avoid targeting victims there. And the same goes for China. I asked Bisping about this. He said it’s true for individuals who live in Russia. “But in Avalanche they ran many parallel campaigns. We also had campaigns which attacked [Russia]. So we have victims [there].” And plenty of perpetrators who weren’t Russian. As for China, “I personally had calls and emails to China and other countries, like Pakistan, where there were normally political issues,” he said. But in this case, “it was necessary [to contact them], and it worked.” He got cooperation. And, of course, it was unlikely that perpetrators who used Avalanche hailed from those countries, though it’s quite possible that zombie computers were located there.

Some of the countries did not want to be named, Bisping acknowledged. And there were political sensitivities. But it wasn’t a hard call for them to participate. “All of these countries were attacked,” he emphasized. “Every country has an interest—a personal interest. Let’s say that every country is losing money. And no country wants to lose money.”

In a way, the gangs that used Avalanche were both a challenge and a model for the coalition that tracked them. If the “good guys” couldn’t demonstrate teamwork at least as effective as the “bad guys,” what would that say?

But Bisping’s point resonated. Self-interest is always a strong motivator. And when individuals, businesses and countries are all under assault by rampant cybercriminals who seem to be operating with impunity, they all have a strong incentive to strike back. But alone, Lange pointed out, they are often hamstrung. Nearly all victims lack resources, or expertise, or both. And it can take a long time to succeed. Even when a country takes the time and spends the money to take down a botnet, a few months later it may be back in business, he added.

In this instance, it took more than four years to defeat the criminals. “In Germany,” Lange said, “even the big cases often have to be closed in six months.” So the lesson here is clear. And it would seem to have implications beyond botnets and cybersecurity. When you’re confronted by an international criminal enterprise, you need an international coalition to respond. “It takes a network,” Lange concluded, “to defeat a network.”

FIGHTING EVEN OVER DEFINITIONS OF FIGHTING

IN SHORT VIDEO CLIPS, A LAW PROFESSOR EXPLAINS WHAT HE BELIEVES ARE GENERAL RULES OF CYBERWAR.

DAVID HECHLER

Is anyone surprised that it's hard to get countries to agree on the rules of war? They shouldn't be. After all, the oldest platitude on this subject is: All is fair in love and war. And that suggests that there aren't any rules.

Surely no one believes that. There are laws, treaties, norms, conventions, general understandings. But don't get too comfortable. The moment you think there's an international consensus, you can be sure that the world will change. A new kind of dispute will arise. Or a technological innovation will introduce a new twist to an old one. And disagreements will erupt again.

Let's start with cyberwar.

Actually, that was precisely what I wanted to do. I wanted to talk to a legal expert on cyberwar. And because this subject is so new, and there's only a provisional grounding on what cyberwar is, and what rules apply, an international group of experts (that's actually what they're called) has been meeting and writing about their efforts to pin this down.

One of these experts is Eric Jensen, a law professor at Brigham Young University, whom I interviewed on Zoom. To give you a quick introduction to the topic, I pulled four short video clips—each under four minutes long. The first introduces Prof. Jensen, who then defines the subject. The second discusses what most experts agree was the first cyberattack that rose to the level of an act of war. The third distinguishes cyberoperations that do not constitute acts of war, and the fourth explains when a nation-state is within its rights to attack the attacker.

If your curiosity is piqued, we invite you to read the entire [interview](#).



Eric Jensen

Video Clips from Our Conversation with Eric Jensen

1. [Defining Cyberwar](#) (3:20)
2. [The First Act of Cyberwar](#) (1:36)
3. [Distinguishing Cyberwar from Cyberoperations](#) (3:45)
4. [What International Law Says About Hacking Back](#) (3:33)



INTERVIEWS



AN INTERVIEW WITH MARK ALBA,
CHIEF PRODUCT OFFICER, ANOMALI

AN INTELLIGENCE-DRIVEN APPROACH TO XDR FROM ANOMALI

The purpose of any extended detection and response platform is to support the translation of data collection into actionable prevention, detection and response. This objective benefits from an intelligence-driven emphasis where all-sourced threat intelligence is analyzed and correlated into proactive defensive actions that optimize returns on investment.

Anomali offers a commercial solution that consists of an intelligence-driven, cloud-native XDR solution for global enterprises. We wanted to learn more about how Anomali supports customer engagement by utilizing all-sourced telemetry to stop breaches and repel cyber threats.

TAG Cyber: What is meant exactly by XDR and how does it relate to threat intelligence?

ANOMALI: An effective XDR solution is vendor agnostic and brings a proactive approach to threat detection and response. It easily integrates into existing environments to deliver visibility across all security telemetry—including endpoint, network and cloud data—while applying analytics and automation to address today’s increasingly sophisticated threats. Our cloud-native open XDR platform provides increased visibility across an organization and its threat landscape to help quickly identify threats in real time by automatically correlating all security telemetry against active threat intelligence to expose known and unknown threats. By correlating the world’s largest repository of global actor, technique and indicator intelligence with our nearly infinite detection capabilities, we can deliver a one-of-a-kind extended detection and response solution that continuously detects threats and prevents attacks before they happen.

TAG Cyber: How does The Anomali Platform work?

ANOMALI: Anchored by big data management and refined by artificial intelligence, our platform is made up of three key components that work together to gather security data from any telemetry source. We then correlate it with our global repository of threat intelligence to deliver high-performance threat detection. First, there is our ThreatStream Intelligence Management system that automates the collection and processing of raw data, transforming it into actionable threat intelligence for security teams. Next is Anomali Lens, a powerful natural language processing engine that helps operationalize

The relentless expansion of the enterprise attack surface will continue to create challenges for security teams and opportunities for their adversaries.



threat intelligence and empower analysts with real-time context to inform their organization and accelerate decision making. Finally, there is Anomali Match, which provides precision threat detection to help a SOC identify and respond to threats in real time by automatically correlating all security telemetry against active threat intelligence, thereby quickly and effectively stopping breaches and attackers. Our platform's suite of components empowers security-operation teams by detecting threats with precision, optimizing response and achieving resiliency. Our SaaS-based solutions easily integrate into existing security tech stacks through native-cloud, multi-cloud, on-premises and hybrid deployments to solve security use cases that aren't addressed by any other solutions on the market.

TAG Cyber: How does your solution support incident response?

ANOMALI: Our platform helps reduce false positives, enabling analysts to cut through the noise by only analyzing, validating and responding to relevant threats. We deliver an increased understanding of the attacker, as well as its techniques and tools, to enable an optimized response. In addition, analysts and incident responders can investigate via an integrated workbench to increase security-analyst productivity in threat research, analysis and finished intelligence publication. They can also automatically associate adversarial tactics, techniques, and procedures (TTPs) and attack patterns with techniques and sub-techniques in the MITRE ATT&CK enterprise framework to identify gaps in security coverage, take action to mitigate these gaps, and prevent follow-on attack stages. Finally, they can automatically disseminate data to other security products via the industry's most extensive set of turnkey integrations for blocking and monitoring—including SIEM, Firewall, IPS, EDR and SOAR.

TAG Cyber: Tell us more about how your customers can prioritize their security investment based on output from your platform.

ANOMALI: Our platform helps elevate response performance and increase return on existing security investments via cloud-native multi-tenant solutions that easily integrate into existing security tech stacks. We provide differentiated insights by correlating all telemetries—the "X" in XDR, extending from endpoints to the public cloud—with the largest repository of global intelligence to help improve efficacy and reduce a security team's workload, while enabling more private and secured community collaboration.

TAG Cyber: Can you share some insights into the future of enterprise threats in the coming years?

ANOMALI: With an increasing dependency on the cloud, along with a growth in digital transformation and remote workforces, the relentless expansion of the enterprise attack surface will continue to create challenges for security

teams and opportunities for their adversaries. Boards and management teams are navigating a complex new terrain of escalated cybersecurity activities, geopolitical uncertainty and macro headwinds, including inflation, at a time when digital transformation is paramount and talent scarcity is at an all-time high. Now, more than ever, management teams need relevant business insights to swiftly protect themselves and their stakeholders from cyberattacks. That is the focus of our open XDR solution: to help management teams amplify visibility; enrich with relevant context; predict an adversary's next move; and, ultimately, stop the attack.



“Let’s leave. I mean, there’s like, no Kubernetes experts here.”



AN INTERVIEW WITH DR. CHRIS PIERSON,
FOUNDER AND CEO, BLACKCLOAK

CONCIERGE DIGITAL PROTECTION FOR CORPORATE EXECUTIVES AND HIGH-ACCESS EMPLOYEES FROM BACKCLOAK

An executive's digital footprint and online presence is one of the new attack surface vectors into a targeted enterprise. The personal devices and home networks of corporate leaders are often not protected, requiring new security solutions to address this risk to avoid attacks on a company.


To minimize cybersecurity risk, BlackCloak provides concierge digital executive protection for upper management, board members and high-risk employees, along with their families. We wanted to better understand the risks originating from personal digital lives, as well as BlackCloak's comprehensive SaaS-based solution that addresses the security and privacy concerns of its clients.

TAG Cyber: How can companies be targeted through the digital presence of their executives?

BLACKCLOAK: The soft underbelly of enterprise security has become the personal digital lives of key employee personnel—in particular, those with access to corporate strategy, confidential information, proprietary data and finances. This is partly due to the normalization of remote and hybrid work, but is mostly the result of cybercriminals identifying a new path of least resistance, allowing them to seamlessly bypass a company's robust security controls. CISOs have done a great job in hardening the corporate environment, and now personal digital lives—including digital privacy, personal devices and home networks—have become the next weakness. We know from our own data that more than three-in-ten executives have malware on their personal devices, while 23% have open ports on their home networks. Additionally, 87% of personal devices are leaking data, and only 8% have MFA installed across all apps, devices and systems. Not to mention, a majority of people still use the same passwords in their personal and professional lives.

All of this presents a huge problem to a company for a variety of reasons. For one, attackers who successfully breach a home network or personal email often have unobstructed green space to move laterally into an organization's digital infrastructure and launch a malware or ransomware attack. Earlier this year, US cybersecurity officials caught Chinese nation-

CISOs have done a great job in hardening the corporate environment, and now personal digital lives—including digital privacy, personal devices and home networks—have become the next weakness.



state hackers doing this very thing with the personal Gmail accounts of high-value workers in critical infrastructure. Many busy executives conduct professional work on personal devices. A breach of any personal device can lead to direct and collateral damage to a business, primarily in the form of financial fraud, reputation damage, business email compromise, account hijacking, unauthorized access and other impacts of consequence. Cybercriminals know that personal devices are highly susceptible to cyberattack and there is very little security teams can do on their own to mitigate this risk; corporate controls cannot be extended into personal lives, due to resource, legal, privacy and ethical constraints, and consumer-grade protections aren't built to withstand advanced targeted attacks.

TAG Cyber: How does the BlackCloak offering work?

BLACKCLOAK: We provide complete, enterprise-grade, digital privacy protection, home-network security, personal device security for mobile and desktop, and incident response via a single SaaS-based platform. Our proprietary technology helps reduce the digital footprint of corporate leaders by removing their personal information from more than 200 data-broker websites. We also scan the deep and dark webs daily for compromised accounts and passwords. We harden privacy settings across all devices, apps and systems to help protect the location and identity of our customers. On devices, we provide XDR technology via an intuitive application that is of a similar caliber to what can be found on corporate phones and computers. We scan devices for botnets and have created our own deception network to trick and trap potential adversaries across all member endpoints. We protect the home through weekly penetration tests, in search of open ports and compromised Wi-Fi. All our technology is backed by a US-based security operations center, offering 24/7 incident response every day of the year. Our white-glove concierge support service answers all customer questions and navigates challenges, while creating a culture of privacy and security.

TAG Cyber: How does your solution work for families?

BLACKCLOAK: Cybercriminals don't care who they hack, as long as it helps them achieve their objectives. Thus, family members of corporate leaders are increasingly at risk. Every week, our team sees a spouse or partner being targeted in an effort to attack the main executive target. And if you think kids are off limits, think again. We protect family members in the same way we protect our corporate clientele.

TAG Cyber: Tell us more about how enterprise teams can engage with you to protect their leaders.

BLACKCLOAK: Most companies recognize that there needs to be a separation between the personal and private lives of

their executives, due to legal, ethical, compliance and privacy concerns. Nonetheless, there are risks that need to be mitigated. When a company decides to use BlackCloak, a set amount of executives, and sometimes their family members, then become BlackCloak members, and we become responsible for their security. To ensure privacy, we never share any personal information with the company. Security teams receive monthly updates from their account rep that are aggregated and anonymized, providing them with an overview of the threat landscape of their executives without having direct visibility into any one person or occurrence. If there is an incident, we collaborate with the corporate security team, providing them with the required information so they can protect the company without compromising an executive's privacy.

TAG Cyber: Can you share some insight into the future of personalized cybersecurity in the coming years?

BLACKCLOAK: We believe that the future of executive protection is digital. As the line between the physical and digital worlds becomes all but indistinguishable, we know that personal cybersecurity will quickly escalate in enterprise and mid markets, going from something that's nice to have to an urgent need. We've already seen this starting to occur; companies that didn't view personal digital lives as an attack vector a year ago are now customers. In addition, we believe that expanded attack surfaces will compel greater collaboration between CISO-led digital security teams and a CSOs physical security teams. After all, ensuring physical security can no longer be accomplished without visibility into the virtual, and vice versa. We also believe that for executive cybersecurity to mature as an industry, it must prioritize privacy by offering the kind of bespoke customer support that high-value individuals are accustomed to in all other facets of their lives.





AN INTERVIEW WITH DAVE KLEIN,
DIRECTOR AND CYBER EVANGELIST, CYMULATE

USING CYMULATE TO OPTIMIZE SECURITY POSTURE

It is no longer sufficient to occasionally scan an enterprise for evidence of possible vulnerabilities. Instead, modern organizations must carefully monitor, manage and optimize their real-time security posture using operational data and advanced breach-and-attack simulation methods.

Cymulate offers a world-class solution for security posture management using continuous validation methods. We wanted to learn more about how the company addresses the needs of enterprise teams when it comes to simulating, evaluating and remediating cyber vulnerabilities and weaknesses that could be exploited by an adversary.

TAG Cyber: What is meant by cybersecurity posture and why is it important?

CYMULATE: Cybersecurity posture is the ability to baseline, trend and thoroughly understand enterprise risk levels from both a business and technical perspective, as well as to empirically discover and test an enterprise to find, prioritize and remediate vulnerabilities, gaps and misconfigurations. There are three reasons why this effort must be continuous and ongoing. First, attackers incorporate new tactics, techniques, procedures and indicators of compromise on a daily basis. Additionally, new vulnerabilities are constantly announced, with exploit times often being only a few hours. Finally, excessive enterprise drift is caused by dynamically changing, complex architectures that are interconnected to a variety of third parties. Several advantages can be gained when cybersecurity posture is addressed through a continuous security-assurance program that safely tests the enterprise against simulated attacks. Executives know they are getting the maximum return on investment for their spend, and that these solutions are aligned to business continuity and cybersecurity, while IT professionals are assured that their security controls, people and incident-response plans are optimized.

TAG Cyber: How does the Cymulate platform work?

CYMULATE: Our SaaS-based Extended Security Posture Management technology helps manage exposure to cyber threats by mapping and blocking possible breach routes, as well as validating the effectiveness of security

Cybersecurity posture is the ability to baseline, trend and thoroughly understand enterprise risk levels from both a business and technical perspective.



controls. It is deployed within approximately one hour, so security professionals can continuously challenge, validate and optimize their cybersecurity posture across the MITRE ATT&CK framework. The platform provides simple, out-of-the-box risk assessments for all maturity levels, as well as a framework to create customized Red and Purple Team Exercises by generating tailor-made, advanced-attack scenarios and campaigns, which are broken into three main categories. First, cybersecurity posture validation is achieved by testing security controls, people, IR plans, SIEM and SOC to learn how well they are performing, as well as to see if they offer protection against the latest threats, and what can be done to optimize them. Next, threat-exposure management is done by running attack-surface management, Red Team automation, attack-based vulnerability management and phishing testing. By doing this, enterprises can accomplish the following: discover known and unknown enterprise digital assets; map and block possible attacker infiltration routes; and ascertain whether an enterprise is susceptible to phishing campaigns. They can further discover vulnerabilities in known and unknown assets, prioritize them, and find mitigating first- and third-party security controls to shore up any gaps between patching cycles. In this way, enterprises gain a smaller attack surface and protection against vulnerabilities, along with better asset management. Lastly, IT security policy enforcement tests look for issues within network segmentation, hybrid-cloud security, and identity and access privileges. Through testing, a company can learn and remediate issues, including: adversarial movement between network segments; cloud environment and identity gaps, leading to improved authentication; and IAM enforcement, segmentation and secure access. All the above is achieved in a manner that is continuous, automated, simple to implement and easy to manage.

TAG Cyber: What steps do you recommend that customers follow to simulate, evaluate and mitigate posture threats?

CYMULATE: We generally see enterprises implement continuous, cybersecurity posture testing in a four-phased, additive approach. Most customers start with security-control optimization and threat assurance, so they know they are secure against the latest threats. Next, they use Purple Team and scenario-based testing to ensure the SOC team and SIEM solution can easily discover and remediate threats as they occur, and that all IR and SOAR plans are working well. Up next are vulnerability management and attack feasibility campaigns. The former allows a company to prioritize and minimize risk and/or vulnerability windows by finding first- and third-party controls that mitigate between patching cycles— all using a process that is easy to maintain. Attack feasibility campaigns include Red

Team automation and phishing campaigns, so an enterprise can find and remediate additional trouble spots, as well as educate and raise cyber awareness. Finally, a company can manage and minimize its external attack-surface risk, as well as test third-party and supply-integration points into the enterprise, in order to sector them off and provide least-privilege access, thereby preventing them from becoming vectors of attack.

TAG Cyber: Tell us more about how enterprise teams can prioritize security decisions using your platform.

CYMULATE: Our solution incorporates both out-of-the-box and user-customized dashboards, testing and outputs—all which include clear-cut prioritization summaries. This is done on both a business and technical impact level. Our customers use this data to prioritize spending and remediate issues, so they can focus on the best existing cybersecurity solutions in their possession, as well as justify new solutions, if needed.

TAG Cyber: Can you share some insights into the future of enterprise security in the coming years?

CYMULATE: Enterprise security is evolving into a partnership between business leadership, technical leadership and cybersecurity vendors. Business will provide business continuity risk valuations; technical leadership will translate that into deliverables; and the cybersecurity vendor will ensure updates on a continual basis. Learn-as-you-use capabilities, along with customizable templates and automation, will make things more manageable. We are witnessing an increased push for interoperable solutions, especially when it comes to sharing intelligence on attacks and vulnerabilities, as well as remediation instructions.



“The board is going to want a more specific number than a kazillion.”



AN INTERVIEW WITH DR. AVIV YEHEZKEL,
CO-FOUNDER & CTO, CYNAMICS

IDENTIFYING THREATS IN NETWORK TRAFFIC USING CYNAMICS

Networks continue to serve as the backbone for modern computing by connecting end users and devices to applications located in data centers and cloud. The traffic associated with such activity will necessarily include evidence of threats, but identifying such evidence is not easy. It requires expert use of AI to be truly effective.

Cynamics provides a commercial security platform that uses deep-learning methods to detect threats using only a small percentage of collected network traffic. We wanted to gain insight into how this is done and how enterprise teams can benefit from this type of protection coverage.

TAG Cyber: What types of threats can be detected in network traffic?


CYNAMICS: Our approach is based on predicting network patterns preceding attacks across different network levels, including gateways, assets, endpoints, etc. As security professionals, we know that cyber attacks and threats are not singular events; they are the outcome of a flow. Each step in this process has a pattern preceding it, and this is what our technology is expert at detecting. Thus, we can detect everything from volumetric attacks—including DDoS, DLP, ransom and scans—to very low-volume stealth web attacks, lateral movements and C&C, as well as new attack vectors uncovered by Cynamics for the first time.

TAG Cyber: How does the Cynamics platform work?

CYNAMICS: Our solution is SaaS-based hosted by AWS—either commercial cloud or GovCloud. It collects small network samples of less than one percent using existing industry-standard sampling protocols and APIs that are built into every type of gateway—sFlow/IPFIX (physical gateways), Netflow (Cisco), VPC FlowLogs (AWS, GCP) and NSG (Azure). From these, conclusions can be made about the full network.

By using small, completely scalable network samples, we can work with any network size or architecture, providing full network coverage and threat detection. We are also completely agnostic to encrypted traffic, due to the fact it doesn't process or analyze the packet payload or data but only the IP-header metadata fields. Onboarding to Cynamics usually lasts a few

Our novel technology automatically activates without any manual intervention. It learns how the full network behaves, discovers network assets and predicts attacks and threats before they happen.



minutes, consisting of a one-time activation that sends network samples without the deployment of any appliance, probe or sensor into the client network, and without any network changes or modifications.

Subsequently, our novel technology automatically activates without any manual intervention. It learns how the full network behaves, discovers network assets and predicts attacks and threats before they happen. The user views everything in a detailed dashboard, where they can investigate threats, set up custom alerts, and run queries and reports. Finally, the user can use our integrations with third-party mitigation tools, so that once a threat is detected, CYNAMICS will immediately forward its root-cause analysis to the mitigator to take action on behalf of the user.

TAG Cyber: How do you utilize AI and deep learning to detect patterns?

CYNAMICS: Our AI technology is covered by several patents and has been featured in many papers published by the world's leading academic conference. Our technology is groundbreaking due to its ability to learn so much from so little data. To date, we have published two pillars of our anomaly detection technology. The first pillar is a new AI concept we invented called "auto-encoder losses transfer learning," which is able to transform the loss vectors of auto-encoders on different client networks into a similar statistical distribution, thus detecting and classifying threats in a generalized way that is agnostic to the specific client. The second pillar is our ability to detect threats at the endpoint without running an agent or EDR by transforming the computer network to graph neural-network learning and the normal behaviors of each endpoint.

We like to call our AI approach the "Google Translate of networks." It translates very different networks into one specific language that our models know very well. Our pre-trained models provide immediate value during onboarding, unlike classical anomaly-detection approaches that need to be trained from scratch over weeks. By normalizing different network patterns into a single language, our AI technology predicts attacks before they hit. Even when not trained on a specific attack pattern, it can predict new "unseen" data based on previous historical patterns. It is continuously learning, evolving, perceiving new patterns and generalizing them. This is unlike existing approaches that look for specific built-in signatures, yet fail to predict new "unseen" attack patterns.

TAG Cyber: Tell us more about how small percentages of traffic are sufficient to gain full visibility.

CYNAMICS: As an organization's network becomes bigger in size, with more data volume and complex architectures, there arises a messy mix between on-prem gateways—such as physical switches and firewalls— and the private and public cloud, including AWS, Azure and GCP. There is no way to analyze one-hundred percent of the packets one-hundred percent of the time, as did legacy NDR solutions. Most NDR vendors use appliances that require spanning and tapping to analyze network traffic. The appliance-based approach doesn't scale; each appliance is limited to a certain amount of traffic, which is negligible when compared to overall network traffic volumes. It can even expand the organization's attack surface by creating backdoors straight to the core of the network.

In today's interconnected digital environment, this approach fails to provide sufficient transparency across increasingly complex smart networks. Organizations need to find a compromise between where to place appliances and the majority of the network that must be left behind, creating one big blind spot for attacks. Samples allow us to cover the full network from end to end without further compromise. It's not easy to make conclusions about a full network based on small network samples. In fact, it is still considered a difficult open challenge in the industry and academy, but we are solving it with our novel technology for the first time.

TAG Cyber: Can you share some insights into the future of network security in the coming years?

CYNAMICS: We believe there will be a rapid move toward sample-based network detection and response. Traditional solutions analyze one-hundred percent of the traffic, one-hundred percent of the time. This was possible decades ago, but with today's exponential growth in network size, volume and architecture complexity, it's no longer feasible. Going forward, next-gen NDR solutions must use sample-based approaches to deal with massive network data, as well as support multiple architectures and environments.



AN INTERVIEW WITH AMIT SHAKED, CEO AND CO-FOUNDER, LAMINAR

SECURING CLOUD DATA USING LAMINAR

Data is obviously the lifeblood of a modern enterprise, but it has undergone a considerable transformation—from being resident in private data centers to increasingly being scattered across a myriad of cloud services. This new arrangement has considerable implications for threat management and compliance.

Laminar offers the first cloud-native data security platform for everything built and run in AWS, Azure, GCP and Snowflake. We wanted to better understand their approach to discovering cloud-resident data, including shadow data, and how their solution could be used to better understand an organization's security posture.


TAG Cyber: What are the primary threats to cloud-resident data?

LAMINAR: Companies have embraced cloud services to provide accessibility, streamline productivity and increase operational resilience for employees working remotely. For most organizations, however, the rapid adoption of cloud services has come with consequences. Visibility has been sacrificed and security compromised in the name of expedience. This complexity and lack of visibility result in unknown, or shadow, data. Recent Laminar research revealed that 82% of data-security professionals struggle with this issue. Examples of shadow data include: unknown data in test environments; cloud data-store backups; remnants of cloud data migration; sensitive data hidden in logs; and embedded databases in compute instances, to name just a few. These unknown data stores often contain sensitive information, such as customer or employee data, financial information, intellectual property, and other classified or confidential information. If left unprotected, shadow data increases the risk of exposure for enterprises, which could result in unnecessary reputational and revenue harm. After all, you can't protect what you can't see.

TAG Cyber: How does the Laminar platform work?

LAMINAR: Our platform is agentless, utilizing native cloud-provider APIs to discover a company's data. It embeds into an enterprise's environment, providing data security for everything built and run in the cloud. Our platform uses the following four steps: discover, prioritize, secure and monitor. First, during the cloud-data discovery phase, it continuously finds, characterizes and classifies known and shadow data across multicloud architecture, organizing it into a cloud data catalogue using our

Enterprises must be prepared. Today about 50% of enterprise data is based in the cloud, and that number will continue to quickly increase over the next few years.



DeepScan technology for both security and governance. Next, risk-based prioritization prioritizes data assets according to sensitivity, volume, data security posture and exposure, as per our risk model. The secure stage provides data security posture management (DSPM), which enforces data security best practices and policy, while guiding remediation and reducing the data attack surface. Finally, we monitor prioritized data access for data-leak protection (Cloud DLP) by uncovering access anomalies in real time.

TAG Cyber: How does your approach support the need for managing visibility into data security posture?

LAMINAR: A major issue today is there is no automated way to understand and verify data security posture; all efforts are manual. Not only that, but, as a first step, you have to know where all your data is in order to assess the security posture—and, when it comes to the cloud, data security teams have fallen behind. With Laminar, the first step is to autonomously discover and classify all of a company's cloud data. We do this without any prior knowledge of the environment. It's a hands-off approach that doesn't need to know anything or bother anyone. Once we discover, classify and catalogue all of a company's data, we then automatically assess risk to prioritize remediation actions based on sensitivity, volume of data, security posture and exposure. All this is done continuously and asynchronously without an agent, so we don't interrupt production data flows.

TAG Cyber: Tell us more about how the Laminar approach integrates into existing IT and security infrastructure.

LAMINAR: Our product is designed for a multicloud environment. The architecture utilizes a cloud service provider's native APIs for complete observability. Our platform brings teams together with the common goal of protecting a company's data. The data-management team integrates with the broader enterprise data-management platform, including: the data security team, by customizing data security policies; the SecOps team, through integrating data security issues and alerts into SIEM or ticketing systems; and, finally, developers and DevOps teams, by integrating with CI/CD tools so timely remediation can occur.

TAG Cyber: Can you share some insights into the future of cloud data security in the coming years?

LAMINAR: Data is no longer a commodity, it's a currency—for both organizations and adversaries, alike. Attacks on cloud data are going to inevitably continue to increase, and enterprises must be prepared. Today about 50% of enterprise data is based in the cloud, and that number will continue to quickly increase over the next few years. We are learning about cloud security and already seeing an increase in data-centric cloud security, adding to existing infrastructure-centric security efforts.



AN INTERVIEW WITH BRAD HIBBERT,
CSO & COO, PREVALENT, INC.

MANAGING THIRD-PARTY CYBER RISK USING PREVALENT

Significant cybersecurity challenges have emerged for enterprise teams, which include operational concerns and compliance issues. A fundamental problem is that enterprises cannot expect perfect visibility into the security ecosystem of suppliers and partners, resulting in risks to data, systems and shared resources.

Prevalent is a leader in providing commercial solutions for managing third-party risks to security and compliance exposure. We wanted to learn more about how this third-party security capability could be deployed to reduce cyber risk.


TAG Cyber: What are some of the key risks that enterprise teams experience with third-party vendors, suppliers and partners?

PREVALENT: Our customers see risks across six broad categories. First, there is cybersecurity, which includes risks to data and systems via outside intrusions through a third party. Next are business risks, such as a third party's lack of resilience when faced with operational challenges or disruptions due to pandemics or natural disasters. Financial risks are when third-party vendors and suppliers experience financial troubles, bankruptcy or have a poor credit rating. Examples of Environmental, Social and Governance (ESG) risks include a supplier having a poor environmental record, being accused of using illegal labor or not practicing overall effective corporate governance. Reputational risks—such as negative news, product recalls, executive misconduct and sanctions—can also be cause for concern. Finally, compliance risks comprise things like GDPR findings, failed audits, bribery, corruption or ethical problems. While cybersecurity and data-protection risks garner the most attention, many of the other risk types carry regulatory weight behind them, too.

TAG Cyber: How does your platform work during the Third-Party Risk Management (TPRM) lifecycle?

PREVALENT: We start by automating the RFP process by adding demographic, fourth-party, ESG, business, reputational and financial insights to help procurement teams incorporate risk intelligence to vendor selection decisions and pre-contract due diligence. Next, we automate the migration of a selected vendor into contracting by centrally tracking all contracts

Because a lot can happen in between regular assessments, we continuously track and analyze externally observable threats to vendors and other third parties.



and attributes with workflow and version control. Once a vendor is selected and contracted, we issue profiling and tiering assessments to calculate inherent risk scores. With this data, companies can categorize vendors and make decisions on the scope of further due diligence.

We also offer a library of more than 100 questionnaire templates and custom surveys to assess third parties on a wide range of criteria—from InfoSec and data privacy to ESG and financial solvency. We take the answers from these surveys and populate a central risk register that can be used to view and act on risks. We also provide reporting by regulation and frameworks to simplify how data is presented, as well as manage remediations down to an acceptable level of residual risk.

Because a lot can happen in between regular assessments, we continuously track and analyze externally observable threats to vendors and other third parties. We help organizations through centralized dashboards that manage and track third-party performance to contractual requirements. Finally, we automate contract assessments and offboarding procedures to reduce an organization's risk of post-contract exposure.

TAG Cyber: What is the role of visibility in third-party risk management and how does your platform optimize such visibility?

PREVALENT: The old maxim is true: You can't manage what you can't measure. And I would add: You can't measure what you can't see. Enterprise risk visibility is at the core of our platform. It starts with procurement—gaining pre-contract visibility into risks like vendor finances, data breaches or compliance problems—and extends to offering a single role-based platform that multiple enterprise teams can use to view the risks that matter to them. We do this through customized, role-specific dashboards and reporting.

TAG Cyber: Tell us more about how you support TPRM through the use of your vendor risk network.

PREVALENT: Our networks are on-demand libraries containing thousands of vendor risk reports that are continuously updated and backed by supporting evidence. Customers use the networks—Exchange, Legal Vendor Network and Healthcare Vendor Network—to get a jump start on their vendor due-diligence process by gaining immediate access to completed assessments, helping them scale their programs so they can shift their time and energy from hounding vendors to identifying and remediating exposures.

TAG Cyber: Can you share some insights into the future of TPRM in the coming years?

PREVALENT: We see TPRM moving towards greater levels of outsourcing, involving more enterprise teams and risk types, as well as evolving to a more continuous model and going deeper in certain industry verticals. First, enterprises rely on an ever-widening network of third parties, while also facing an expanding web of geopolitical risks, regulatory requirements and cybersecurity threats. Unfortunately, most companies manage these risks by using manual processes that place a greater emphasis on risk identification than risk remediation. Over the next several years, organizations trying to scale effective TPRM risk programs will hit a wall, causing them to adopt more automated and proactive approaches, such as leveraging external business process outsourcing firms and/or dedicated purpose-built external TPRM software.

Next, enterprises are being pressured by a range of stakeholders—including regulators, investors and consumers—to improve visibility and oversight of their exposure to third-party risk. While organizations may begin by focusing primarily on cyber threats, they will see the need to enable risk-based decisions by proactively assessing and monitoring a more comprehensive risk profile throughout the third-party relationship. This will require the rationalization and harmonization of technology, processes (workflow) and people.

Departments and teams will need to consider risk in all activities and decision making, including activities that are currently more focused on operational efficiency. Teams responsible for everything from sourcing and onboarding new vendors to managing their performance over time will continue to consume risk intelligence from similar data sources (e.g., a comprehensive risk profile) and begin to leverage insights from their peers in supporting contract negotiations and discussions related to their respective workstreams.

Enterprises will also continue to enhance third-party programs by utilizing integration, automation, intelligence networks and analytics to continuously assess and monitor their extended supply chains more closely. Finally, enterprises in certain verticals will continue to adopt sharing networks to accelerate risk identification and place a greater focus on risk remediation. These sharing networks will evolve beyond assessment sharing to intelligence sharing as enterprises and third parties design, embrace and enforce open communication to proactively share insights related to cyber, compliance, incidents, performance and more.



AN INTERVIEW WITH MARIO VUKSAN,
CEO AND CO-FOUNDER, REVERSINGLABS

DETECTING THREATS AND REDUCING SUPPLY CHAIN RISK USING REVERSINGLABS

Malware continues to generate risks for enterprises, causing them to struggle as they sift through software, databases, files, web content, emails and storage for evidence of problems. World-class tools and expertise are required when investigating and hunting for malware, especially in the event of a software supply chain compromise that requires binary analysis.

ReversingLabs is a world leader in deep-threat analysis and software assurance. We wanted to learn more about how the ReversingLabs solution works, as well as how it helps customers address modern cyber threats and reduce the risks associated with the software supply chain.


TAG Cyber: What is meant by deep software and file threat analysis?

REVERSINGLABS: Software is different from source code. It consists of binary components packaged into either one file, or a collection of files, under the same umbrella. Each component is likely a binary conversion of the original text-based programming language script. Downstream consumers of that software binary, however, have little or no information as to how it was constructed. At the same time, attackers are increasingly exploiting vulnerable software supply chains to gain access to sensitive environments. This is where deep software analysis comes in. Deep analysis is necessary when no information about the file and software is available. Reverse engineering is, therefore, necessary to understand the intent of the inspected content. The goal is to identify potentially malicious features and functionalities that may be lurking within the binary. Early detection of such tampering can prevent downstream attacks and the resulting financial and reputational damage. ReversingLabs is a recognized leader in deep threat analysis and software assurance, with expertise in identifying software supply chain threats and attacks.

TAG Cyber: How does the ReversingLabs platform work?

REVERSINGLABS: We specialize in understanding binary content. To do this, we first collect all relevant primary source materials related to a software application, including: the accurate identification of software components and subcomponents; the extraction of structured data; the locating of secrets; and the identification of known malicious behaviors,

Attackers are always focused on obtaining the biggest reward for the least amount of effort, causing them to gravitate toward software and platforms with the widest possible reach.



vulnerability indicators and network indicators, to name a few. Building upon this primary source material, we generate an explainable threat classification for any source files. This analysis allows us to generate full reports on software assurance and the supply chain for both software and containers.

TAG Cyber: How does your solution support supply chain risk?

REVERSINGLABS: We believe that all software needs to be thoroughly inspected for the presence of malicious intent, tampering, software quality, leaked secrets or unwanted network indicators. This is true regardless of whether the software is developed in-house or by third parties, contractors, outsourcing firms or offered as open source software. We do not rely on the collaboration of software authors to assess supply chain security, making us unique among software supply chain security firms. Instead, we provide an independent assessment of supply chain risk by analyzing binary components, software installers, libraries, containers and virtual machines (VMs) that are products of the development process. We are the last line of defense for software publishers, and the first line of defense for software users, reliability engineers and DevOp teams before a software is accepted or installed. Our secure.software platform provides detailed insights into complex software packages by identifying important markers of software quality, as well as describing the state of those markers, thereby enabling the efficient management of related security risks for organizations of any size. For example, our secure.software platform can compare two versions of the same software and detect changes introduced between them. Those changes might cover a wide range of software quality issues, including behavior changes that affect the packaged software components. Our platform recognizes tens of thousands of different behaviors, while providing highly detailed, granular insights into the capabilities of the analyzed software. In this way, any malicious software components can be quickly pinpointed and sanitized.

TAG Cyber: Tell us more about how your platform can assist the threat hunter.

REVERSINGLABS: We assist threat hunters by providing tools and intelligence for exploring complex binary content. Our technology can inspect payloads extracted from network flow and email, as well as those found in storage, containers and software applications. We give threat hunters the power to correlate a new class of evidence with log, email and netflow data using custom and community signatures. Moreover, our analysis tools work regardless of the binary complexity or the number of layers of obfuscation used. For example, our researchers recently discovered a widespread software supply chain attack involving more than 30 malicious JavaScript modules that were

being distributed as free, open source components via the Node Package Manager (npm) package repository. They contained malicious code that was surreptitiously stealing form data from applications and websites that used the malicious packages, which were look-alikes of legitimate and widely used npm packages. Our analysis began with the identification of malicious, obfuscated code in these modules, which uncovered a far-reaching campaign involving malicious command-and-control infrastructure used for exfiltrating data and managing malicious modules. These indicators of compromise—including malicious, look-alike domains and packages—can be used by threat hunters to identify compromised systems within an organization.

TAG Cyber: Can you share some insights into the future of malware and software security in the coming years?

REVERSINGLABS: Software supply chain threats carry the largest possible blast radius for organizations. For example, the SolarWinds attackers gained access to the environments of 30,000 downstream customers by infecting a single product with a malicious back door. Similarly, even obscure npm libraries might be used by thousands, or ten of thousands, of individual development organizations. A single compromised or malicious npm module that is implemented in tens of thousands applications can expose tens of millions of downstream users to attack. Attackers are always focused on obtaining the biggest reward for the least amount of effort, causing them to gravitate toward software and platforms with the widest possible reach. Defenders need to be attuned to that risk and start verifying the software infrastructures that they have historically trusted blindly. Even simple efforts to harden software and verify the integrity of software supply chains will go a long way in reducing the attack surface of applications, helping organizations to protect sensitive data and insulate themselves from legal and reputational risks.



“Happy to serve you, Master - but first I’ll need proof of identity.”



AN INTERVIEW WITH MIKE KISER,
DIRECTOR, STRATEGY & STANDARDS, SAILPOINT

HOW ENTERPRISE TEAMS CAN ACHIEVE IDENTITY SECURITY USING SAILPOINT

As enterprise leaders drive their computing infrastructure toward a greater use of cloud, the need to ensure the highest levels of identity security becomes a critical requirement. Achieving this objective demands automation in order to streamline identity-related processes, as well as enable secure access, privilege management, collaboration and other tasks.

SailPoint provides world-class identity management and governance for enterprise teams. We wanted to learn from this industry leader about how identity security integrates with cloud evolution and how the core components of its platform can be used to avoid the growing risk of identity breach.


TAG Cyber: What are the lifecycle management requirements that must be addressed in any identity security platform?

SAILPOINT: The entire lifecycle of identities must be secured and governed by the platform—from their creation and transformation over time to their eventual retirement or suspension. This governance includes more than just awareness, however. Identities and their attributes must be trusted, especially when they inform subsequent policy. To support identity-centric security strategies such as zero trust, it is essential that the identities are only granted access when they need it and ensure that old access is removed as the role of the identity evolves. As an identity is sunsetted, all access must be removed in a time-appropriate manner. Finally, it's important to remember that this identity lifecycle has to be supported for all identities—machine, business partner, RPA—and not merely for human identities.

TAG Cyber: How does the SailPoint platform work?

SAILPOINT: Our platform delivers identity security to an enterprise by providing visibility and AI-assisted governance. This process commences with discovery and visibility into all places where identity is present in the organization. Often, this starts with drawing from authoritative sources—key repositories, such as HR, that are at the core of a business. As our Identity Platform encounters new applications, troves of sensitive data or repositories for identity, they are correlated back to a single view per identity—called an “identity cube”—that provides a single view of all attributes, access and, when possible, activity for that identity. This allows us to see all relationships between identities and their access, as well as the

Our platform delivers identity security to an enterprise by providing visibility and AI-assisted governance.



usage of AI and ML, in order to build up an appropriate access model for the organization. This model is used to ensure that access is appropriate, both in terms of usage and policy. In this way, the business is enabled by leveraging economies of scale, while risk is reduced through the checking of higher order policy, such as the separation of duties and the like.

TAG Cyber: How does SailPoint use AI to drive identity-related security?

SAILPOINT: As noted in the previous question, we initially build an identity cube for each identity in the system by centralizing information about the identity, including its access and activity. Our identity platform then uses graph-based algorithms to find groups of affinity or likeness. These groups establish what is normal for the organization, and this can then be used to create an appropriate access model. The system can then utilize this information to grant automatic access, when appropriate, based on the identity context. It can also begin to recommend the correct response to users responding to certifications or access requests. Explainability of these recommendations is key, as it builds trust in the system rather than asking for blind acceptance. As the platform matures, the AI/ML model becomes more intelligent in these decisions and, eventually, is able to take over most of the necessary decision making. Edge cases will still be presented to human users to resolve new situations or potential gray areas.

TAG Cyber: Tell us more about how compliance management is supported by SailPoint.

SAILPOINT: Compliance with regulations and standards—proving that the organization is doing what it claims to be doing—is always an essential piece of identity security. Auditors in certain industry verticals are looking for evidence to ensure that the correct decisions are being made and that poor choices are mitigated. But it's not just auditors who should be interested in compliance: Executives and board members must be personally vested in ensuring that these processes are carried out, as it reduces risks to the business.

Our identity platform has long been focused on providing collateral to support the evaluation of compliance with policy and industry standards. The automation provided by newer technologies such as AI/ML holds great promise, as it lightens the load when demonstrating the fulfillment of an organization's claims. We have been in constant conversation with the auditors, executives and boards of the enterprises we serve, and we look forward to working together to drive these ideas further.

TAG Cyber: Can you share some insights into the future of identity security in the coming years?

SAILPOINT: Over the next few years, identity security will continue an evolution that started a decade ago and has intensified over the last few years. This evolution has been marked by three key characteristics of identity: ubiquity, autonomy and ease of use. First, in regards to ubiquity, identity is no longer an afterthought, as it is included in every new system, device and program. This ubiquity also means that all systems within an organization must understand and be able to communicate coherently about identity and identity context. Securing organizations is—and has always been—a team sport. Secondly, autonomy will become a key element of any identity security platform. The aforementioned explosion in the scale of identity means that systems must use innovation to keep up with the ever-changing environment. Humans have been outstripped by the current state, and this will only continue. Finally, ease of use will reign supreme. Humans must be channeled into making good identity security choices; this will only happen if the best option is also the one with the least resistance from the end user. Identity security will evolve along these lines over the next decade. Consequently, we are investing in ubiquity, autonomy and ease of use in partnership with our customers.



“Let’s upgrade our software to Version III.VI.X”



AN INTERVIEW WITH BOB LAM, CEO AND CO-FOUNDER, SHARDSECURE

IMPLEMENTING CLOUD DATA FRAGMENTATION FOR ENTERPRISES USING SHARDSECURE

The shift to hosting and storing data in the cloud brings new risks to enterprise teams. These include the possibility that cloud-service insiders with access to data could create data-leakage conditions.

ShardSecure offers an effective solution to this problem that involves the sharding of data into fragments. We wanted to learn more about how this new method can be effectively deployed to improve data resiliency.


TAG Cyber: What is data resilience?

SHARDSECURE: We look at the CIA triad—confidentiality, integrity and availability—as the three pillars of data resilience. At the risk of sounding hyperbolic, data is the lifeblood of most organizations. It must be kept safe from prying eyes, yet be available to the appropriate users at all times. Its integrity must be maintained, which means being free of all kinds of tampering.

TAG Cyber: How does your solution work?

SHARDSECURE: We use a three-step process of shred, mix and distribute. First, we shred data down to four-byte microshards. The purpose of getting down to that size is to make the microshards too small to contain a complete Social Security number, driver's license number, birthdate, or what have you. This effectively desensitizes the data. We then mix those microshards with poison data into logical containers. The purpose here is to make any unauthorized re-assembly virtually impossible. Lastly, the microshard containers are subsequently distributed across multiple, customer-owned storage locations that may include hybrid- and multi-cloud environments. Now imagine that one of those storage locations was compromised or improperly configured. An unauthorized user would have only an indecipherable fraction of the complete data set with no knowledge of where the remaining pieces were or how to re-assemble them, as well as what is poison data versus what is legitimate, and so on. A key component of microsharding is self-healing data. The simplest way to think of it is like RAID-5 for your data in the cloud. Self-healing data helps to maintain data integrity. It

Even someone with access to all storage locations would have enormous difficulty identifying which of those logical containers correspond to any given file, because we strip file names, file types, metadata, etc.



neutralizes ransomware, while including data availability so that users may still operate unimpeded during a service outage or security incident.

TAG Cyber: How does microsharding address insider risk for cloud administrators?

SHARDSECURE: All of the above-mentioned complications that an unauthorized user would face just to locate, let alone make sense of, microsharded data is applicable to any type of rogue insider. Even someone with access to all storage locations would have enormous difficulty identifying which of those logical containers correspond to any given file, because we strip file names, file types, metadata, etc. And if that rogue insider were to tamper with or delete any microsharded data, the above-mentioned, self-healing data performs multiple data-integrity checks, reconstructing any affected data to its original state should there be a failed data integrity check. Really, data at rest should never be directly modified or deleted in any way. If that does happen, that's an indicator of compromise. So, we'll also alert the SOC and/or feed alerts to a SIEM, SOAR, or what have you for incident response purposes.

TAG Cyber: Tell us more about how your solution would be deployed to multicloud infrastructure.

SHARDSECURE: From a deployment perspective, it's pretty straightforward, as we're entirely software based. Each instance is a virtual cluster that can be deployed in any cloud environment and/or on-prem. Multiple instances may be set up as standalone deployments or synchronized for load balancing, high availability and fail over. For backend storage, we use customer-provided storage in a multi-cloud, multi-region or hybrid-cloud environment. We also make it straightforward to migrate data between storage locations, whether it's between different regions with the same cloud provider, between cloud providers, or between the public cloud and on-prem. The important part to note is that these kinds of moves don't require application downtime and can take place at any time the data owner wishes.

TAG Cyber: Do you have any predictions about whether cloud data fragmentation can play a role in future global cyberwars?

SHARDSECURE: We have a great deal of confidence in the role that cloud data fragmentation can play as a powerful means of data security, particularly as part of a robust defense-in-depth strategy. We receive quite a bit of positive feedback on this approach when we speak with customers and prospects. Looking at the number of competitors in the space, the active investing they and we have received, and the fact that TAG Cyber has created a segment for cyber defense frameworks, we believe all these are signs of a strong future for this space.



AN INTERVIEW WITH LISA UMBERGER,
CEO, SICURA

HOW SICURA SUPPORTS COMPLIANCE ACROSS IT, OPERATIONS AND DEVOPS

Compliance demands require that all levels of staff and management in an enterprise's IT, operations, security and DevOps divisions coordinate their security approaches. The DevOps lifecycle is the most demanding aspect of this required cooperation, since continuous compliance is required during high-velocity agile software development.

Sicura provides a commercial solution for such continuous compliance, with an emphasis on the assurance of system integrity for operating systems and other software systems. We wanted to learn how this solution works and how enterprise teams could integrate the platform into their protection ecosystem.

TAG Cyber: *Tell us about SIMP and how your solution evolved from this approach?*

SICURA: I spent 12 years at the NSA, running cybersecurity and compliance for hundreds of systems, along with a staff of security engineers. My biggest challenge was keeping systems secure and compliant over time. We would build a compliant system, but as soon as it was out in the world and being interacted with by humans, it was immediately out of compliance. A regular scan would reveal major compliance issues, and we'd issue 500-page reports to the engineering teams so they could manually remediate those problems. In 2009, we were using a new change management tool called Puppet, which allowed us to continuously monitor and manage environments at the server level. We leveraged that technology as a vehicle for monitoring and enforcing compliance. Instead of engineers having to manually fix the individual issues revealed by a scan, we could automate that process to continually enforce and remediate issues over time. We called the product the Server Integrity Management Platform, or SIMP. In 2015, we worked with the NSA to open source SIMP through the Technology Transfer Program. We built a commercial version of the product, which would later become Sicura, because we believed that private enterprises require the same level of security and compliance as the government. At Sicura, we're on a mission to automate security and compliance so that the organizations powering the world's critical technology systems can operate securely and efficiently.

We're on a mission to automate security and compliance so that the organizations powering the world's critical technology systems can operate securely and efficiently.



TAG Cyber: How does the Sicura platform work?

SICURA: Our platform ingests existing compliance and security standards, generating a configuration that is directly applicable to systems. It then automates the enforcement of those standards across server and cloud environments. The product enforces a number of government- and industry-standard policies, such as the Center for Internet Security (CIS) Benchmarks, the Defense Information Systems Agency's Security Technical Implementation Guides (DISA STIGs), and the technical portions of the new Cybersecurity Maturity Model Certification (CMMC) requirements. We do this via a three-step process: assess, enforce and remediate. First, we use an open-source or commercially available scanner to assess the status of a system and compare that to the requirements of the policy, or policies, an enterprise wants to adhere to. Next, we enforce those policies by revealing every place where a system is out of compliance in a digestible, actionable format—reports are no longer than 500 pages. Finally, we remediate by showing exactly what needs to be changed to return to compliance; these changes can be implemented either automatically or with the click of a button.

TAG Cyber: How does your solution support continuous compliance?

SICURA: Our solution can be used for one-time compliance remediations, as well as for continued enforcement of compliance settings across infrastructure. We leverage Puppet as one of our supported technology platforms to achieve continuous compliance. Using this approach, we enforce a defined compliance policy in regular 30-minute intervals, while automatically remediating non-compliance for any server or system configuration. As continuous verification is a key component of any zero trust framework, it is crucial to ensure that compliance policies are continuously enforced. Organizations using Sicura can be confident they are meeting important policies and standards at all times, without fear of security drift or non-compliance. By continuously enforcing compliance, organizations can guarantee that they are putting the security of their trusted partners first.

TAG Cyber: Tell us more about your platform's target users or customers within a typical enterprise.

SICURA: Our solution is an engineering product that achieves security goals. Therefore, our primary customers sit in the engineering, cloud, infrastructure or server divisions of large enterprises with legacy infrastructures and strict requirements for security and compliance. Our users are engineers and system admins, as well as their managers. We alleviate the pain points felt by engineers and system admins who hate

the tedious, time-consuming work of manually remediating security issues, while also helping their managers and leaders achieve more with fewer resources, by allowing engineers to refocus on solving big-picture engineering problems. In a public case study, the IBM Federal Cloud Team estimated that Sicura increased their efficiency by 85% in the first year, saving them over two million dollars. Moreover, we also serve security, compliance and IT divisions. Security teams appreciate our console's ability to provide continuous insight into an organization's security posture, and compliance teams can be assured that an organization is always audit-ready, as the system is constantly being assessed and improved with Sicura. Finally, IT and operations can make pre-approved changes to the system with a click of the remediate button, without risking downtime or unintended consequences.

TAG Cyber: Can you share some insights into the future of software security in the coming years?

SICURA: We believe that zero trust security will be the most common model for designing applications and systems, as well as accessing those systems. Traditionally, zero trust models aim at continuously verifying access and limiting reach should a breach or unintended access occur. As this model expands into the designing of systems, organizations will seek to limit their exposure to unnecessary third parties when developing and protecting supply chains. Instead, they will rely on verified software—either through trusted partners who can guarantee and prove compliance to known standards, or through software that they can verify internally to eliminate the need for external risk and exposure. As standards such as CIS Benchmarks continue to evolve and cover more software, a greater number of organizations will be able to verify full-stack compliance and demand higher standards from all external sources they integrate with. Continuously verifying and enforcing these standards will become the norm in a zero trust environment.



AN INTERVIEW WITH ERIC KEDROSKY,
CISO, SONRAI SECURITY

COMPREHENSIVE CLOUD PROTECTION USING SONRAI SECURITY

Currently, enterprises are shifting to the public cloud, offering a great promise of agility, innovation, accessibility and lower costs. These benefits come with a significant increase in responsibility to ensure that a proper range of controls are in place to protect cloud-resident data and workloads. Sonrai Security provides a holistic approach to protecting cloud deployments using a unified commercial platform.

We wanted to gain insight from the Sonrai Security team as to how this approach addressed cloud risk for their customers, and how it employs controls focused on workloads, identities and data.

TAG Cyber: What are the primary cloud risks that your solution addresses?

SONRAI SECURITY: We believe identity and data must be at the foundation of every organization's security strategy, and our platform was created specifically with this in mind. We assess the four main pillars of cloud security: platform misconfigurations; workload vulnerabilities; data-access and exposure risk; and identity risks, such as separation of duty, toxic combinations, over-privileged identities and privilege escalation. These do not work in isolation, but all influence each other. Our unique ability to tie all these pillars together—as opposed to addressing them in silos—allows businesses to view their cloud risks in context.

TAG Cyber: How does the Sonrai Security platform work?

SONRAI SECURITY: We deliver enterprise cloud security for the public cloud that other solutions miss. Powered by our cloud identity graph, Sonrai Security Dig combines workload, platform, identity and data security in one platform. Best practices, workflow, advisors and automation support cross-team cloud-security operations. Our mission is to unearth, prioritize and remove risk across every part of a customer's public cloud, by offering complete and total visibility into all compute, identity and datastore activity. We connect the dots by finding and eliminating relationships that create toxic risk, unwanted access and lateral-movement opportunities for attackers. Our graph shows every way an identity gains privilege or access to data. Customers are able to prioritize their concerns using our platform, which eliminates meaningless alerts going to the

wrong teams. The platform can automatically configure security controls tailored to unique workloads based on their business impact and risk level. Finally, we help customers operationalize and remediate issues quickly with bots, workflow and team accountability.

TAG Cyber: How does your solution integrate with the on-going journey toward greater cloud adoption by most enterprise teams?

SONRAI SECURITY: Organizations choose our platform as the foundation of their cloud security operations, whether they're fully cloud or in the midst of a digital transformation. Modern app development has eviscerated traditional security controls and created unique risks that current tools can't handle. We believe that when done correctly, the cloud delivers security far better than anything possible on prem. Sonrai Security Dig was built to tackle cloud complexity, and its ability to view identity and data risk in context is at the core of our product. Cloud means an explosion in roles and identities. As an organization's cloud footprint grows, the complexity becomes unmanageable. The cloud begs for a new method of triaging a flood of alerts, requiring cloud, security, DevOps and audit teams to unite together. Finally, cloud means a multitude of cloud accounts, roles, service principles and data stores, all of which need to be secured.

We help reveal risks companies didn't know they had, by connecting the dots between identities, data, workloads and platform, and then remediating them at the speed and scale the cloud demands. By breaking down the silos between the pillars of cloud security, organizations obtain a level of context that allows them to prioritize concerns and operationalize remediation.

TAG Cyber: Tell us more about the workload security aspect of your solution.

SONRAI SECURITY: Knowing the age, CVSS score and exploit status of business risks is not enough to prioritize the vulnerabilities in an organization's environment. Recognizing which vulnerabilities are the most dangerous to a business means understanding threats unique to the host. Detecting workload vulnerabilities is just the first step. We examine connected platform, identity and data risks to reveal the full severity of workload vulnerability. We use analytics and proprietary risk amplifiers to highlight vulnerabilities with increased concerns, including sensitive data access, and over-privileged or exposed identities that could allow for lateral movement if that vulnerability were exploited.

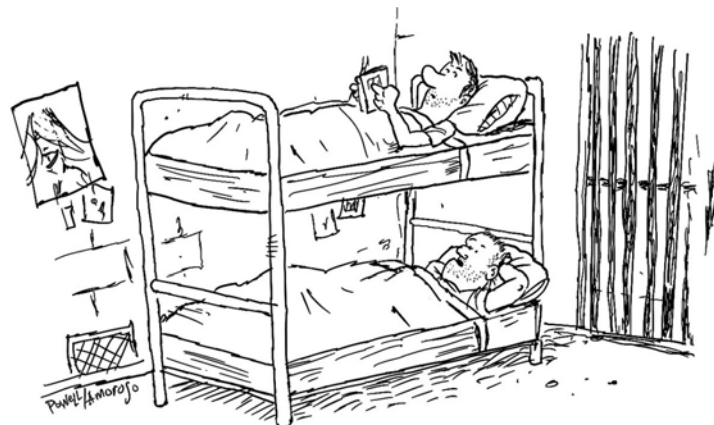
Our lightweight agentless scanner discovers a full host inventory without impacting performance or cloud spend. This helps

enterprises get a clear picture of what every host is connected to, and who (or what) can access it—or already has. This allows teams to spend less time on hardening, configuration, network firewalling and micro-segmentation tasks. If a business already has a scanner in place, we offer alert prioritization with host-specific risks to further enrich the solution. Our ability to de-emphasize vulnerabilities without impacting sensitive data is one of our key capabilities, because we know the average team is drowning in security concerns.

TAG Cyber: Can you share some insights into the future of cloud security in the coming years?

SONRAI SECURITY: We strongly believe identity and data must be the foundation of every cloud-security strategy, and an organization's main goal should be protecting their data. Identity and data-access complexities are exploding in the public cloud, along with an array of interdependencies and inheritances that first-generation security tools miss, as shown by so many data breaches in the cloud. This is going to drive CIEM to the top of a CISO's list of must-haves. Cloud adoption is going to expand rapidly. This will increase the attack surface, resulting in more malicious attacks. Increasingly sophisticated bad actors are growing alongside the cloud. Their attack methods will shift towards targeting cloud environments, expanding past simply targeting a public bucket or exploiting a VM vulnerability. This is why it is so urgent for organizations to get a hold on their security now, before things get completely out of hand.

To survive, organizations will have to adopt automation, which is the only answer for solving security concerns at the speed and scale of the cloud. Automation has been noted as a tool to leverage in the past years, but many organizations are hesitant to lean into it. Finally, the prominence and impact of data breaches has changed the role of the CISO. It will soon become fundamental to have CISOs on the executive team and in boardrooms.



“I never guessed lateral traversal would get me here.”



AN INTERVIEW WITH TSACHI GANOT,
CO-FOUNDER AND CEO, SUNDAY SECURITY

PROTECTING EXECUTIVES FROM CYBERTHREATS WITH SUNDAY SECURITY

Every prominent individual on the internet worries about being targeted by cyberthreat actors. This risk is particularly relevant to high-profile executives whose persona is closely linked to the corporate brand.

Sunday Security is a start-up offering solutions in this area. We asked them to share insights into how their platform protects individuals from targeted threats.


TAG Cyber: Explain how the online digital personas of executives and board members can introduce risk to an enterprise.

SUNDAY SECURITY: Senior executives, high-profile business leaders and other key personnel have significant online digital presences. A recent study showed that in 2020, 94% of Fortune 500 CEOs were on LinkedIn, and 62% had profiles on Facebook, YouTube or Twitter—up from 39% just five years earlier. It is possible that the pandemic contributed to this increased use of public platforms, but the trend is unmistakable. The threat that emerges is transitive: An organization is dependent on some key person; that key person has established and maintains an online digital presence; and malicious actors use this presence to target the individual and, in turn, the organization. This is an important new exploitable surface that many organizations have simply not factored into their overall attack surface management (ASM) approach. The goal, therefore, is to protect online accounts from being targeted for weakness. The power of a single account being compromised cannot be underestimated. For example, a recent attack by the Lapsus\$ hacking group used limited access from a single compromised account. This illustrates the power of offensive actors to target the mismanaged presence of a single individual.

TAG Cyber: How does your solution work and what type of protection do you offer?

SUNDAY SECURITY: The online identities of a company's executives directly represent and impact its brand. Our solution provides a three-layered digital executive protection program for key individuals within an organization.

Our SOC benefits enterprises that want a total separation of the personal and the professional by outsourcing personal incidents to a third party.



The first layer of protection is our proprietary personal SaaS Security Posture Management (SSPM). Taking inspiration from the enterprise security world, we've built our own version of an SSPM for personal accounts, including Google, LinkedIn, Twitter, iCloud, etc. Our SSPM continuously scans all connected, personal online accounts for known vulnerabilities, analyzing hundreds of data points across these accounts. Essentially, we're running a continuous penetration test on digital identities, evaluating vital signs, such as MFA, password security, connected devices, recovery methods, third-party permissions, etc. This access allows us to evaluate security-related data in an unsoiled fashion—not as an account, but as an identity. The second layer of protection is our enterprise platform, which was built to help security teams understand and quantify their exposure to the personal attack vector. Ever wonder what percent of your executive teams are using MFA or rotating their passwords? Or how many board members are walking around with leaked passwords or a malicious email-forwarding rule? Our enterprise solution aggregates data from the end-users SSPMs, allowing the CISO to understand the exposure represented by the executive team and key personnel, without violating their privacy or gaining any access to their accounts.

Finally, the third layer of protection is our own personal SOC, which we manage directly out of our offices. The purpose of our SOC is twofold. First, many organizations prefer not to get involved directly in personal cybersecurity incidents; our SOC benefits those who want a total separation of the personal and the professional by outsourcing personal incidents to a third party. Secondly, our SOC supports an executive's personal cybersecurity needs on all fronts—from a spearphishing email to their personal account or a suspicious friend request on LinkedIn to a ransomware attack on a personal device. These are not typical enterprise security incidents, and we think the proper way to deal with them is a dedicated off-prem resource.

TAG Cyber: How can executives, boards and their families also benefit from this type of protection?

SUNDAY SECURITY: Executives, board members and their families find themselves in the crosshairs of cyberattackers, who target their personal online identities in order to reach the enterprise. Our solution provides best-in-class cybersecurity for these vulnerable individuals, while also maintaining their privacy. Cybersecurity awareness alone isn't enough to stop sophisticated attackers.

TAG Cyber: Do you have any predictions about how the personal cybersecurity market will evolve?

SUNDAY SECURITY: As the consumer cybersecurity market continues its slow and steady decline, I believe enterprise cybersecurity will eventually swallow up the consumer market—thereby moving the responsibility for personal cybersecurity to the enterprise. Furthermore, I think we could see a future in which executives—and maybe even employees—are vetted for cybersecurity purposes during the onboarding process. They could also be offered a cybersecurity solution and cyber insurance as part of a benefits package, in the same way that healthcare plans are currently provided. Additionally, a person’s personal digital identity could be leveraged to improve cybersecurity from an IAM perspective. If you already have a good understanding of someone’s personal devices, accounts, locations and networks, can that data then be used to enhance authentication on the enterprise side? It’s still too early to determine, but the possibilities are pretty exciting.



“I’m sorry, honey - but there is no “like” button for real life.”



AN INTERVIEW WITH ARTI RAMAN,
FOUNDER AND CEO, TITANIAM

A NEW APPROACH TO DATA PROTECTION FROM TITANIAM

As data flows through an enterprise, it must be protected from a variety of different threats, ranging from unauthorized access to ransomware. The use of encryption has always been a primary control in this regard, but it has impeded the ability for search, analysis and other important, fully authorized tasks.


Titaniam provides a new cybersecurity mechanism that protects enterprise data through a variety of different methods, including support for encryption-in-use. We wanted to learn more about their suite of flexible data-protection solutions, as well as how enterprise teams can use it to reduce cyber risk.

TAG Cyber: How does the Titaniam platform address the challenge of data protection?

TITANIAM: We offer a data-security platform that is designed to address tough data-protection challenges. We offer the industry's only high-performance, petabyte-scale, encryption-in-use solution. It comes in a single platform combined with nine other traditional data-security and privacy techniques, providing protection even under the most difficult circumstances—such as when admin privileges get compromised or when trusted insiders attack from within. In addition, we provide the industry's richest Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) capabilities, which let data owners hold and control encryption keys without impacting the functioning of shared applications. Our encryption-in-use retains full data usability, including search and analytics. The solution attaches to a wide variety of data platforms and applications, ranging from object and relational stores to file systems. Our five interoperable modules can be mixed and matched to cover a large variety of cloud and hybrid architectures.

The best way to understand why these capabilities are important is to take a closer look at the data-protection challenge itself. Enterprise data protection is a four-part challenge. First, there is the challenge of volume and variability. Enterprises have enormous amounts of data scattered across many data platforms and applications. As the data grows, it is copied and distributed much faster than an organization's ability to identify, classify and protect it. Our solution supports the breadth of data platforms, as well as variability in architectures, allowing

Moving forward, enterprise data exfiltration and extortion is going to become the primary mission in the majority of cyberattacks.



a company to execute an effective data-protection strategy. Second is the privacy-versus-usability challenge. Enterprises now use vast amounts of automation and data-driven decision making. This huge amount of data must be available to the business for active use. Traditional data protection in the form of encryption and tokenization is at complete odds with this need. Any sort of protected data is basically unusable, because when it is called for use, it needs to be decrypted and detokenized. This is either completely impractical or so slow at scale to be unviable. Our solution supports rich data utilization, including full-featured search and analytics, while retaining encryption and other privacy-preserving formats.

Next, challenges arise when trusted paths are breached. Modern-day attackers do not hack into systems, they simply log in. In a world of stolen credentials and identities, data-security technologies cannot tell the good players from the bad. In order to protect data under such circumstances, our protected solutions do not yield clear text even when accessed with highly privileged credentials—not in the index, queries, memory or search results. Clear text is computed if dictated by policy, but it is never persisted. Finally, there is the challenge of critical mass. With multiple copies of data being spread out and scattered across an organization, a data-protection solution must protect enough data to prevent compromise in a meaningful way. As data flows through an enterprise, our platform extends protection across systems, allowing for shared data context, schemas, key infrastructure and more.

TAG Cyber: Tell us more about how your solution supports encryption-in-use.

TITANIAM: We offer what some would consider an engineering solution to the encryption-in-use problem. We integrate into data platforms, as well as modify search and indexing processes to work with encrypted data. By facilitating this type of encryption-in-use, we can support database querying operations on sensitive data without decrypting it anywhere—not in storage, indexes, memory, etc. Our protected systems stand up to attacks that target large-scale data exfiltration via admin accounts. We offer encryption-in-use for structured and unstructured data. Moreover, our encrypted data supports complex searches, such as prefixes, suffixes, wildcards and more. The core technology can be extended to perform pattern matching on images and videos, as well as sound-based matching on audio files.

TAG Cyber: Does your solution address privacy enforcement for enterprise customers?

TITANIAM: One of our key value propositions is that when data leaves a Titanium-protected data platform, it can be released in

nine different privacy-preserving formats, including: traditional and format preserving encryption; vaulted and vaultless tokenization; full or partial; static or dynamic masking; redaction and hashing. This functionality is available at a granular level, as well as for whole indexes, collections or files. The same data can be sent to different downstream systems in a variety of privacy-preserving formats. Privacy policy can be tied to existing application Role-Based Access Control (RBAC). In this way, Titanium makes privacy enforcement very efficient.

TAG Cyber: How is third-party data risk addressed by your solution?

TITANIAM: We provide two significant capabilities that address third-party risk. First, data being processed by third parties can retain encryption at all times, including while in active use. Decryption operations can be tightly controlled via policy, permissions or specific case-by-case approvals. Second, if data does reside with third parties, the data owner can utilize our HYOK to retain encryption keys. These keys can be turned off at any time or otherwise restricted to limit what a third party can do with the data.

TAG Cyber: Can you share some insights into the future of enterprise data security in the coming years?

TITANIAM: It is our belief that moving forward, enterprise data exfiltration and extortion is going to become the primary mission in the majority of cyberattacks. Attacks are going to become less about disruption and system lockup, which can be messy and result in capture, and more about quietly stealing data and selling it, or extorting it for profit. In this world, zero trust data security is going to be equated with zero clear text. If zero clear text is the goal, then solutions built on encryption-in-use capabilities will become the only viable form of protection.



“5G is such a nice option up here.”



**ANALYST
REPORTS**

INTRODUCING CLOUD DATA FRAGMENTATION (CDF)

EDWARD AMOROSO

The resiliency of cloud-hosted data can be optimized through a fragmentation process, resulting in a distributed representation that is effective against cyber threats such as insider attacks from public cloud hosting teams. Prominent commercial vendors supporting this capability are included in the report.

Introduction

Enterprise data security is best achieved in the context of the organizational mission. For example, banks that handle sensitive customer records must implement controls that prevent this data from being read by unauthorized parties. In contrast, industrial factories that depend on stored machine telemetry and configuration files require controls that prevent such data from being tampered with or altered.

One data security requirement that aligns with many different organizational objectives involves the need to ensure the resiliency of cloud-stored data. Companies that export sensitive or critical files and records to public cloud or SaaS services now require that such data be protected from disclosure, integrity, or blocking threats to the third-party infrastructure. These threats could result from external attacks or cloud service insiders with administrative access.

In this report, we introduce a new category of commercial data security method known as *cloud data fragmentation (CDF)*. The protection strategy that underlies modern CDF platforms and their practical implementation involves breaking up data into discrete components that can be separated, processed, and stored in diverse locations. The approach is well-suited to scattering fragments or shards of data into multiple public clouds.

The CDF concept is introduced and explained below from the perspective of an enterprise security practitioner team with responsibility to protect important data being used across hybrid infrastructure, including use of the major public cloud services. Several commercial vendors are also listed and shown to provide good options for IT and security teams looking to purchase a platform that can be integrated into their local cyber risk framework.

What is Data Resiliency?

Stated simply, data resiliency references how well your data holds up to cyber threats. For many years, the term would include the caveat that resiliency is all about dealing with integrity threats, but with new techniques such as CDF, resiliency can be extended to the disclosure threat as well. This is a profound advance because it addresses the oft-claimed challenge that once viewed, data confidentiality cannot be restored.

The idea behind data resiliency in a CDF context is that distributed objects are more difficult to attack than combined ones. A common non-technical analogy illustrating the concept is that it is much easier to knock over an elephant with a large truck than it is to knock over a swarm of mosquitos. The truck might hit a small subset of the bugs, but no matter what it does, the majority will evade being targeted. This visual image can be extended to data resiliency.

Specifically, data stored in public clouds can be distributed across different storage domains to improve its resiliency. The algorithms for breaking up the stored data must obviously be designed to support not only the distribution of the data, but also reassembly when the data is needed. In addition, it must provide support for the various tasks that might be performed on the individual pieces including encryption.

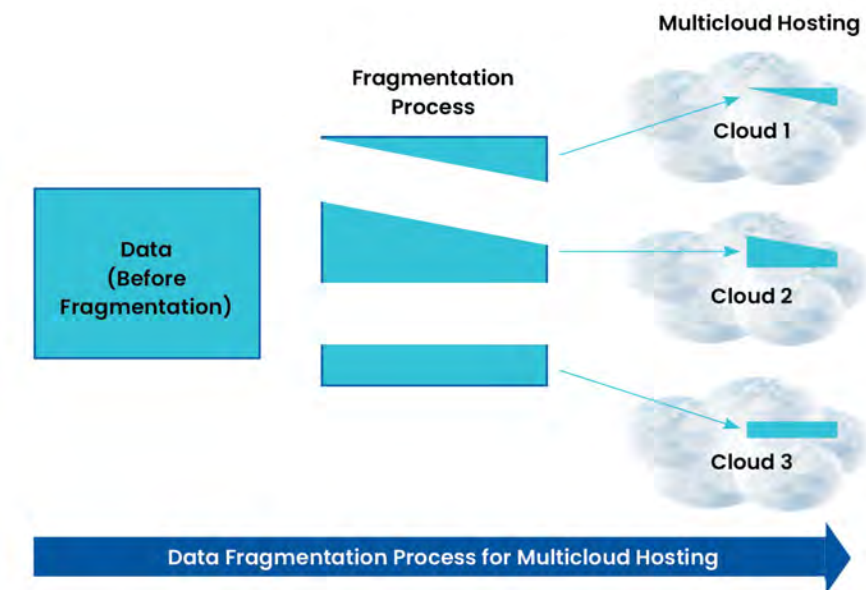


Figure 1. Distributing Data to Multiple Clouds to Improve Resiliency

The general method of distributing data has been in existence for many years, and infrastructure providers have considerable experience fragmenting data for the purpose of data storage control and optimization. It is only recently, however, that commercial vendors have emerged that allow for such distribution to be performed at the application level via CDF into multiple clouds to address cyber threats.

What is the Insider Risk for Cloud-Stored Data?

When sensitive data for some significant enterprise or agency is being hosted into a public cloud service, this engagement would be guided by a data hosting agreement. For example, if some large bank decides to use Amazon Web Services (AWS) for hosting of its sensitive data, the respective security teams from the bank and the cloud provider would work through the details of an agreed-upon set of controls for the cloud environment.

It is important to note that, in stark contrast, any mid-sized or smaller company using a public cloud service will have to accept whatever commercial terms and conditions are published by the provider. These might be acceptable or not, but the customer will have little or no options other than comparing the services of another provider. Microsoft and Google, for example, will not negotiate terms of its data hosting with anyone other than a massive buyer.

As a result, the risk emerges that a customer's cloud hosted data might be mishandled either accidentally or deliberately by an administrator working on behalf of the provider. Intentional compromise of hosted data might come from a disgruntled or coerced person with privilege to access hosted data. This is a non-trivial risk because insiders are tough to identify and cloud service providers offer a natural means for such bad actors to access valuable data.

To that end, cybersecurity controls, whether procedural, policy-based, or functional, must be put in place to avoid such insider risk. Typical methods are listed below, along with their respective pros and cons:

- *Multi-Person Controls* – By requiring multiple individuals to participate in the approval that some data-related action be taken, the risk of an insider is reduced to those cases where sufficient collusion is present.
- *User Behavioral Analytics* – Monitoring the behavior of insiders provides a means for highlighting activity that does not match their normal profile and that prompts deeper review and analysis for potential data misuse.
- *Cloud Data Fragmentation* – Breaking up data into fragments and scattering the pieces removes the possibility of an individual cloud service administrator with privileged access having the means to gain unauthorized access to hosted data.

Obviously, all methods for reducing insider risk are recommended, but it should be evident that the use of multi-person controls and user behavioral analytics has not been sufficient to reduce data risk in most environments. For this reason, the new technique introduced here known as cloud data fragmentation (CDF) represents a high-priority functional control that can complement these more mature means for addressing cyber risk.

How Does CDF Work?

The technique of cloud data fragmentation follows the general technical strategy outlined above for distributing data. At a high level, some data element, usually represented as a file, artifact, binary, or other resource, is subjected to a process in which it is fragmented into pieces. This process is also sometimes referred to as a data sharding activity, where the sharded pieces are derived from the whole using some algorithm.

While it would seem obvious, the fragmentation process must in fact represent a function whereby the original data can be reconstructed or interpreted from its pieces. Furthermore, the process must not involve data loss as is found in some compression algorithms that optimize storage for large files such as multimedia. Instead, fragmentation must preserve the essential properties of the original file while also creating shards for separate placement.

The steps involved in most commercial implementation of CDF include options for the IT, cloud, or security team to select based on local requirements. As such, a stepwise conditional methodology emerges for CDF that includes the following commonly found decision steps:

Step 1: Data Fragmentation

In this first step, an algorithm is used to break up the data into fragments. Different vendors will decide on the size of the individual shards (e.g., four bytes), and the use of compression in this step is a common approach. As standards emerge for CDF, one would expect more commonality in the algorithmic paths taken in this step.

Step 2: Data Packaging

The second step involves packaging the individual fragmented shards using an algorithm that might introduce salted or poisoned data. While such adjustment of the data helps with confidentiality, it is usually not a full encryption step. This step can, however, include native encryption as part of the packaging.

Step 3: Data Distribution

The third step allows for distribution of the fragments into whatever targeted infrastructure is desired by the user. This might include cloud storage services, hybrid cloud, or even legacy storage infrastructure. Configuration will be handled by the user, in conjunction with the public cloud services being used.

Step 4: Data Access

This step involves accessing the fragmented data via collection, unpackaging, and combination of the stored shards. It is a design decision whether the pieces are ever arranged back into an aggregate physical object or are just maintained separately for access. Any over-the-top encryption that might have been imposed on the fragments must be addressed here as well.

Certainly, the methodology associated with CDF will vary between enterprise teams (e.g., some adding additional encryption) and also across the major cloud service providers or legacy IT hosting team. In addition, the CDF vendor will play a prominent role obviously, and in the next section, we outline some prominent cybersecurity vendors, mostly start-ups, that offer acceptable capability in this area.

Who are the Prominent Vendors Supporting CDF?

As part of our research at TAG Cyber, we interview cybersecurity vendors including start-ups, and then create customized strength, weakness, opportunity, and threat (SWOT) analyses based on our investigation. This information is integrated into our Research as a Service (RaaS) portal which is used by enterprise teams, vendors, and investors around the world to inform their own source selection of the best vendors for their specific mission.

Using this research base, we offer below a brief summary of the vendors we found to be offering solutions consistent with our introduction of CDF in this report. Considerable additional detail on these vendors is available to TAG Cyber RaaS customers including tailored support for specific questions or challenges being addressed by an enterprise or other team. The summaries below should thus be used as a starting point for CDF planning.



Business Information: Paul Lewis serves as founder and CEO of Calamu. Prominent advisors include John Stewart, former SVP Chief Security & Trust Officer for Cisco. Headquartered in New Jersey, the company recently raised a \$16.5M Series A round of funding.

Brief Solution Description: The Calamu Protect platform supports securing data at rest in a highly scalable and resilient geo-fragmented cloud environment called a data harbor. Calamu offers an agent called Calamu Drive for Windows and MacOS which provides transparent protection for user endpoints. Calamu Drive monitors file activity, performing encryption and fragmentation as needed, and then stores the protected fragments in the data harbor. Calamu Connectors provide API-based integration with premise and cloud-based workloads and databases, providing the same encryption, fragmentation, and storage features as the endpoint agents. Finally, the Calamu Console provides administrative access to the data harbor to enable management of storage and users and to monitor the health of agents and API's.

COHESITY

Business Information: Mohit Aron serves as Founder and CEO of Cohesity. Investors include Sequoia Capital, Wing Ventures, SoftBank, and others. Headquartered in San Jose and founded in 2013, the company completed a Series D round of \$250M in funding in 2018.

Brief Solution Description: The Cohesity Helios solution protects enterprise data with machine learning-based backup and data deduplication through four vertical solutions. Cohesity Helios SaaS provides consolidated archive for premise and cloud-based enterprise data. The Data Management as a Service solution offers data backup, consolidation, disaster recovery, and governance across storage platforms. Cohesity DataProtect supports autonomous backups of critical workloads with SLA support within the workflow toolset, thus providing global search and restore, storage space efficiency, and ransomware protection. Cohesity SmartFiles offers native integration with NAS, SMB, and S3 file storage solutions, enabling near real-time file redundancy. The Cohesity SiteContinuity supports disaster.



Business Information: Michael John Gaffney serves as Chair and CEO of Leonovus. Headquartered in Ottawa and trading on the Toronto Stock Exchange and TSX Venture Exchange (TSXV: LTV), the company was founded in 2010.

Brief Solution Description: Leonovus Smart Filer automatically moves infrequently used data to less expensive cloud storage, thus leaving a symbolic link in its place. Smart Filer leverages any combination of cloud storage offerings and provides access to archived files as if locally stored. The Leonovus Vault provides a FIPS140-2 encrypted certified storage vault. The Vault shreds the encrypted vault container and distributes the data fragments across multiple clouds to ensure data sovereignty and confidentiality. The Leonovus XVault is a byproduct of the Vault, but one focused on secure file sharing. XVault allows enterprise teams to store files in the same highly secure manner as the Vault, but allows them to grant specific user access, thus providing a secure Dropbox mechanism.



Business Information: Steve Wray serves as CEO of Myota. Founded in 2017 and headquartered in Pennsylvania, the company raised \$3.65M in funding in 2021 in a Series A2 round led by investor Ira Lubart.

Brief Solution Description: The Myota solution is a cloud-only file management and data governance platform that chunks, encrypts, and shards critical files to provide both security and redundancy. Any file that is uploaded to the service is chunked, encrypted, and sharded within the Myota infrastructure, with a link provided back to the end-user. Key features supported by Myota includes protection of unstructured data with encryption, shredding of data to render them unusable by third-party administrators or insiders, spreading of data to various repositories to avoid extortion and ransomware, and enablement of data recovery in the event of an attack targeting the resiliency of critical enterprise data. The solution integrates with anti-malware platforms, data leakage prevention solutions, and cloud storage.

SHARDSECURE

Business Information: Bob Lam serves as CEO and co-founder of ShardSecure. Prominent technologist and ShardSecure co-founder Lou Steinberg, former CTO of TD Ameritrade, serves as chairman of the company. The company closed an \$11M Series A funding round in May, 2022, led by Grotech Ventures, Gula Tech Adventures, Tom Noonan, and KPMG in addition to EPIC Ventures, Industrifonden, and Sinewave Ventures. (Full disclosure notice: Dr. Edward Amoroso participates as an unpaid advisor to Lou Steinberg's firm which funds and advises ShardSecure.)

Brief Solution Description: ShardSecure offers on-premises and cloud-based solutions that shred, mix, and distribute enterprise cloud data in multi-cloud and hybrid-cloud environments. The solution's self-healing data offers protection of data from cloud-based ransomware attacks and other data breaches. Once a file has been microsharded, the solution will rebuild that file if any unauthorized attempts of modification or deletion are detected, neutralizing cloud storage ransomware attacks and bolstering business continuity. Additional use cases include secure cold storage migration to the cloud, Microsoft 365 privacy and security, and secure cloud adoption.



Business Information: Ben Golub serves as CEO of Storj. Founded in 2015 by Shawn Wilkinson, who also serves as Chief Strategy Officer, the Atlanta-based company has over 70 employees working in many different countries. Storj is an Ethereum token.

Brief Solution Description: Storj is an open-source software development platform that enables developers to encrypt, shard, and distribute objects across public or private cloud containers. The solution is primarily intended for video streaming, software distribution, decentralized backups, and integration into cloud-native apps. The Storj software development kit (SDK) consists of three primary components, the Uplink CLI, the S3-compatible Gateway, and the Storj client Libraries. Additionally, several pre-built integrations have been developed for Fastly, FileZilla, MongoDB, Duplicati, and Filebase. Many different offers exist for developers to obtain low-cost access to cloud storage.

Action Plan for Enterprise

Enterprise teams considering CDF for sensitive data are advised to create a local initiative to begin planning. While plans will vary between different groups, we recommend that the following steps be included in whatever process is being used to integrate CDF into existing and planned sensitive data storage architectures and associated cloud hosting processes.

Step 1: Data Storage Inventory

Developing an accurate view of the data being stored in legacy, hybrid, and cloud infrastructure is an obvious first step in any plan to integrate CDF. This should include third-party storage and should separately identify SaaS-based data, which is usually not in scope for present CDF solutions.

Step 2: Data Security Policy

Creation of policies for data marking and categorization is important because not all data will likely be subjected to the fragmentation process. Without clear prioritization policies, CDF will be unevenly applied in an ad hoc manner. Instead, it should be a required step for data that rises above some criticality threshold.

Step 3: Vendor Selection and Test

The selection of vendors should be informed by the list included in this report, but enterprise teams might have other options, including developing the method internally. As always, TAG Cyber analysts are available to assist buyers in this important source selection process, usually leading to a proof-of-concept (POC) test.



NEXT-GENERATION VULNERABILITY ASSESSMENT AND PATCH MANAGEMENT: AN OVERVIEW OF ACRONIS CYBER PROTECT CLOUD

EDWARD AMOROSO

Vulnerability assessment and patch management are foundational cybersecurity tasks that have evolved toward next-generation coverage of multicloud infrastructure, data center virtualization and zero trust architectures. The Acronis Cyber Protect Cloud platform is shown to effectively implement these important controls.

Introduction

Despite the many changes that have occurred over the years in cybersecurity, many traditional protection approaches have remained as important and effective as ever. Two complementary examples are vulnerability assessment and patch management. As organizations continue to shift toward virtualization, zero trust and multicloud infrastructure, proper attention to vulnerabilities and patches helps to ensure consistency with cyber risk objectives.

In this report, we review the best current approaches to this combined activity, which we dub VA/PM—and prepend the moniker “next generation” to highlight the evolution of these capabilities to handle multicloud infrastructure, virtualization, zero trust and many other attributes of modern enterprise networks. The Acronis¹ Cyber Protect Cloud platform is shown to effectively implement this next-generation vulnerability assessment and patch management (NG-VA/PM) approach, especially for service providers.

Importance of VA/PM

Keeping track of vulnerabilities and patches is hardly the most exciting aspect of modern cybersecurity, but it could arguably be viewed as one of the most important tasks in an IT risk program. Security breaches often result from exploitation of vulnerabilities that could have been removed, or from patches that were not applied. So the combined task to address these issues has clear implications for cyber risk.

As such, every team responsible for security, regardless of size or sector, must have some means of tracking and prioritizing vulnerabilities, and of ensuring the timely application of patches. The ability to ensure high-integrity support with fail-safe operation is also highly desirable. For example, according to one research survey, 88 percent of companies claim that they would apply patches more quickly if they had the option to unpatch, if necessary.²

It is worth mentioning that VA/PM is particularly important for managed service providers (MSPs), because of their scope. That is, as nearly all SMBs rely on service providers to assist in operating and protecting infrastructure, software and services, their overall cyber risk can be significantly reduced if the service provider handles this task properly. This is one of the great benefits, in fact, of working with a capable service provider.

Challenges of VA/PM

One major challenge for VA/PM involves the existence of known and unknown vulnerabilities. It is reasonable to assume that a large VA/PM program would have good coverage of known, reported vulnerabilities—but it is not reasonable to expect that this will extend to unknown, zero-day problems. In most cases, teams become aware of zero-day exploits only after they have been used in an actual campaign.

An additional coverage challenge, which is arguably more intense, involves the existence of known and unknown assets in an organization. That is, most nontrivial organizations have an incomplete understanding of their asset inventory. As a result, for any vulnerability, it might be unclear whether it actually applies to the local environment. These two unknowns, vulnerabilities and assets, can be represented in a conceptual matrix (see Figure 1).

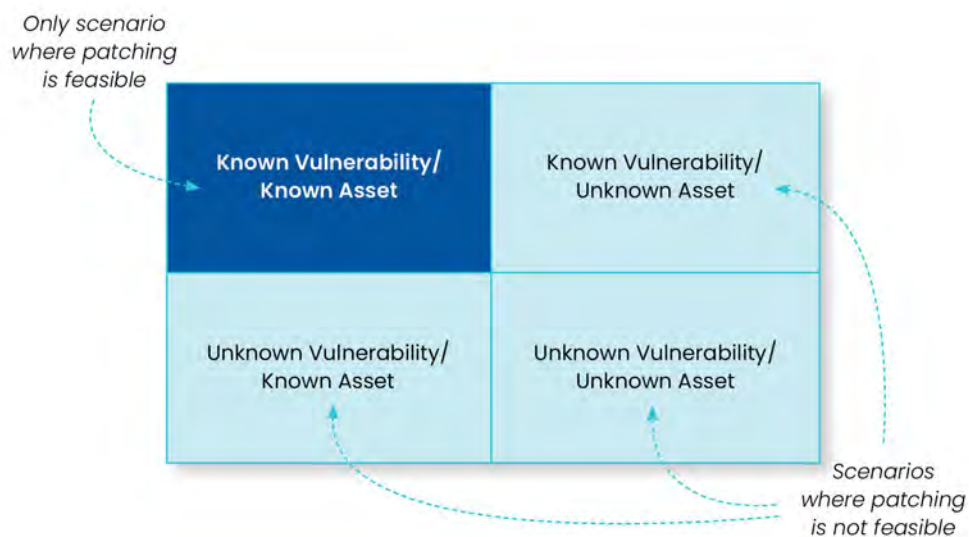


Figure 1. Matrix of Vulnerability/Asset Scenarios

The matrix highlights how important it is for vulnerabilities to become well-known quickly, and for assets to also become known accurately and quickly. These next-generation requirements help to explain how NG-VA/PM has come to be—namely, to ensure that organizations wanting to maintain more accurate and complete coverage of vulnerabilities and patches have sufficient means to achieve this critical security objective.

Modern NG-VA/PM Requirements

The cybersecurity community well understands the vulnerability management challenge and its adjacent tasks of prioritizing and patching (including for non-Windows products). NG-VA/PM is all about making these familiar processes more intelligent, manageable, automated and complete. The specific types of next-generation continuous security functions that are required in this area include the following:

- *Vulnerability Assessments*—Teams responsible for security must have the ability to collect, catalog and manage an accurate list of applicable vulnerabilities. This is best done using global threat monitoring and alerting from multiple sources.
- *Prioritized Patching*—Security teams must use analytics and threat intelligence to determine which patches to prioritize. This analysis requires accurate asset management and inventory, and good external threat intelligence.
- *Forensic Analysis*—NG-VA/PM programs must support future analysis and investigations by archiving vulnerability-related data and associated patches. This allows for more accurate case analysis.
- *Fail-Safe Patching*—NG-VA/PM programs must support the ability to roll back patches if necessary and to ensure high-integrity patch application.
- *VA/PM Compliance*—As with all aspects of modern cybersecurity, NG-VA/PM includes the obligation to support compliance goals. This often involves the automatic generation of reports for external auditors and regulators.

As suggested above, the progression to next-generation capability for VA/PM includes driving intelligence, automation and completeness. It also, however, involves extending applicable techniques, tools and processes to handle the modern transition to new infrastructure, such as public cloud, mobile networks and perimeterless zero trust environments. In the next section, we use the commercial Acronis platform to illustrate how this can be done in practice.

Case Study: Acronis Cyber Protect Cloud Platform Support for NG-VA/PM

The Acronis Cyber Protect Cloud commercial platform is designed specifically to enable MSPs to provide next-generation vulnerability management and patching support for enterprise customers of all sizes around the world. As such, it serves as an excellent use case to demonstrate how NG-VA/PM requirements might be implemented in a live production environment, where a cyberthreat might have significant consequences.

Cyber Protect Cloud includes a range of capabilities that directly address antimalware, patching, virus scanning, backup, vulnerability assessment, sensitive data protection and application controls. MSPs can rely on these capabilities to address safety, security, authenticity, privacy and accessibility requirements among their SMB customers in the context of processes for backup and recovery, security management and antimalware (see Figure 2).



Figure 2. Acronis Cyber Protect Cloud

The primary advantage of combining these functions into a commercial platform is that it helps to streamline the complexity of many different processes and functions. The many challenges inherent in the coordination, combination and integration of the various processes shown in Figure 2 should be obvious. Coordinating backups with antimalware, for example, is one of the great difficulties in dealing with advanced ransomware attacks.

The implication for managed security service provider teams is that an integrated commercial platform such as Acronis Cyber Protect Cloud will likely simplify and streamline the overall NG-VA/PM infrastructure and associated processes for enterprise customers. This is an essential task, especially in organizations with considerable size and scope. Attention to simplification will continue to grow as a requirement in emerging compliance environments.

Action Plan

AMSPs are advised to take immediate action toward implementing a modern NG-VA/PM program using a suitable commercial platform and associated set of processes—such as with the Acronis solution. This can be achieved by following a simple four-step management plan. Each of the four high-level steps obviously must be decomposed into more granular tasks, but the overall approach should be as follows:

Step 1: Inventory of Existing VA/PM Approaches

The head of security and his/her team should create an accurate inventory of existing approaches to identifying, documenting, assessing, prioritizing and closing vulnerabilities. In larger firms, this is likely to include many disparate approaches, tools and processes.

Step 2: Development of NG-VA/PM Requirements

Once the inventory has been established, the security team should create a set of NG-VA/PM requirements along the lines of the functions discussed in this report. The requirements should combine the best elements of approaches identified in the inventory.

Step 3: Commercial Platform Scan and Review

The next step involves scanning and reviewing available platforms such as Acronis Cyber Protect Cloud for suitability in the customers' environments. TAG Cyber analysts can assist with this task, which must take into account nonfunctional considerations such as license terms and cost.

Step 4: Begin Gradual Transition and Integration

The final management step involves transition and integration of the newly selected platform into the local NG-VA/PM ecosystem. The good news is that the types of tasks included in this area are highly conducive to a smooth transition.

¹ Switzerland-based Acronis GmbH (see <https://www.acronis.com/en-us/>) supported and participated in the preparation of this technical report.

² Opatch Survey Report, 2018. <https://0patch.com/>



AUTOMATING CYBERSECURITY POSTURE ASSESSMENT: AN OVERVIEW OF THE BALBIX PLATFORM

EDWARD AMOROSO

Establishing cybersecurity posture is an important step toward mitigating the cyber risks to an enterprise. Automation is the best approach for such assessment—one that builds on existing foundational security methods. The Balbix¹ Security Cloud is shown to automate this cybersecurity posture assessment process effectively.

Introduction

A major goal for enterprise security teams is to identify the attack surface that malicious adversaries can exploit. Such identification is the first step in mitigating cyber risk, and while the process might be simple to define, it is much tougher to implement. Modern enterprise infrastructure typically includes a complex mix of on-premises, cloud, SaaS, and hybrid infrastructure connected via proprietary and off-the-shelf software apps.

The process of defining all relevant vulnerabilities (or lack thereof) for a given attack surface is often referred to as the *security posture*. As one might expect, this has traditionally been achieved using a combination of scanning tools, asset databases, penetration test results, and other security tool output. Aggregation of this data has typically been done manually, often using proprietary algorithms and methods.

In this report, we explain how cybersecurity posture assessments can be automated. This is an important objective because it can establish a more continuous view of posture and will greatly reduce the possibility for coverage or completeness deficiencies. The commercial *Balbix* platform is used to illustrate how such a practical, automated assessment can be done in an enterprise context.

Security Posture Foundations

The challenge of establishing security posture can be visualized by mapping the assets of an organization against potential attacks. The two-dimensional structure that emerges is further complicated by the consequences, expressed in terms of financial loss,² that can result from a compromise. The result is a three-dimensional structure with a massive number of asset-attack-consequence mappings.

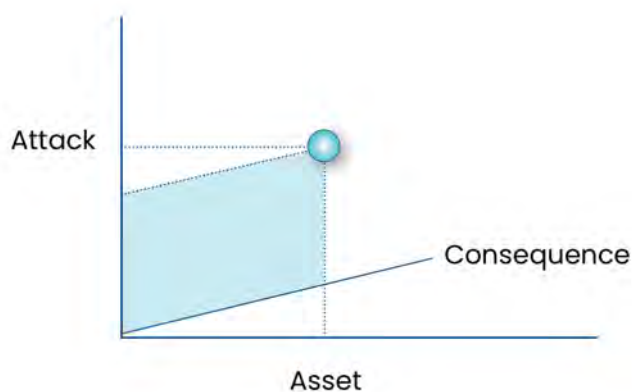


Figure 1. Mapping Assets, Attacks, and Consequences

The goal of gaining visibility into the present and ongoing status of cybersecurity controls is obviously not new. The primary means by which this goal has been addressed in the past includes familiar methods, many of which remain useful, but none of which have properly met the challenge. Since these traditional methods play a role in more evolved strategies for posture assessment, it is worth briefly reviewing the benefits of each.

Breach Simulation

One way to demonstrate the effectiveness of internal controls is to test them continually. To that end, so-called breach and attack simulation (BAS) tools have emerged to help enterprise teams determine the effectiveness of deployed security systems and tools. BAS implementations typically involve placement of active agents on either side of a control to continually test its ability to block attacks.

The advantages of a BAS approach include automated operation and continuous coverage. The disadvantages include limited flexibility and difficulty expanding to include more complex attack campaigns. Ultimately, BAS solutions are likely to find their way into a target security architecture, either as stand-alone platforms or as functional components of a more comprehensive protection architecture.

Vulnerability Scans

An additional major aspect of security posture assessment involves scanning networks, systems, and other resources for evidence of exposure. Operating a security scanner is perhaps the most familiar and traditional aspect of vulnerability detections and, as such, it is not only a requirement in every framework, but is also a major expectation of executives, board members, and other influencers.

The primary advantage of vulnerability scans is the familiar, mature data output that can support existing security and compliance programs. Most participants in enterprise security expect and understand this data, so scanning is essential in this context. The primary disadvantage is that scan data is prone to gaps in coverage and significant misinterpretation by executives and other stakeholders.

Penetration Tests

Penetration testing is also an effective means for identifying security vulnerabilities, especially ones that are subtle and not easy to find. For many years, enterprise security teams have relied on expert white hat hackers to probe, scan, and explore visible infrastructure with the goal of finding exploitable errors before a malicious adversary might find them and cause real consequences.

The advantage of penetration testing is that it is good at identifying the presence of security issues. That is, in environments where it is not generally accepted that exploitable holes exist, penetration testing can provide clarity. The biggest problem with penetration testing, however, is that it is an insufficient means for demonstrating the absence of problems. Not finding something during a penetration test doesn't mean that it doesn't exist.

Crowdsourced Testing

Finally, the use of vetted hackers (e.g., bug bounty) to help identify vulnerabilities has been an important component of an enterprise security posture assessment program. Since techniques, skills, and insights can vary so much between expert testers, having a large group of such individuals targeting a given system is a major advantage that offers depth of coverage and scope that cannot be reached by an individual.

The advantage of crowdsourced testing is the wide range of skills that can be harnessed to identify exploitable vulnerabilities. A drawback, however, is that considerable time and effort is required to properly vet and manage the ethical hackers. This workload can be mitigated through partnership with a capable commercial vendor, but it nevertheless represents a considerable hurdle.

The challenge with these various methods is that while they each provide some degree of visibility into security posture, they remain disparate and uneven in terms of their automated or manual control. In the next section, we introduce a commercial platform from Balbix that uses automation as the basis for establishing an accurate, scalable view into the security posture of an organization.

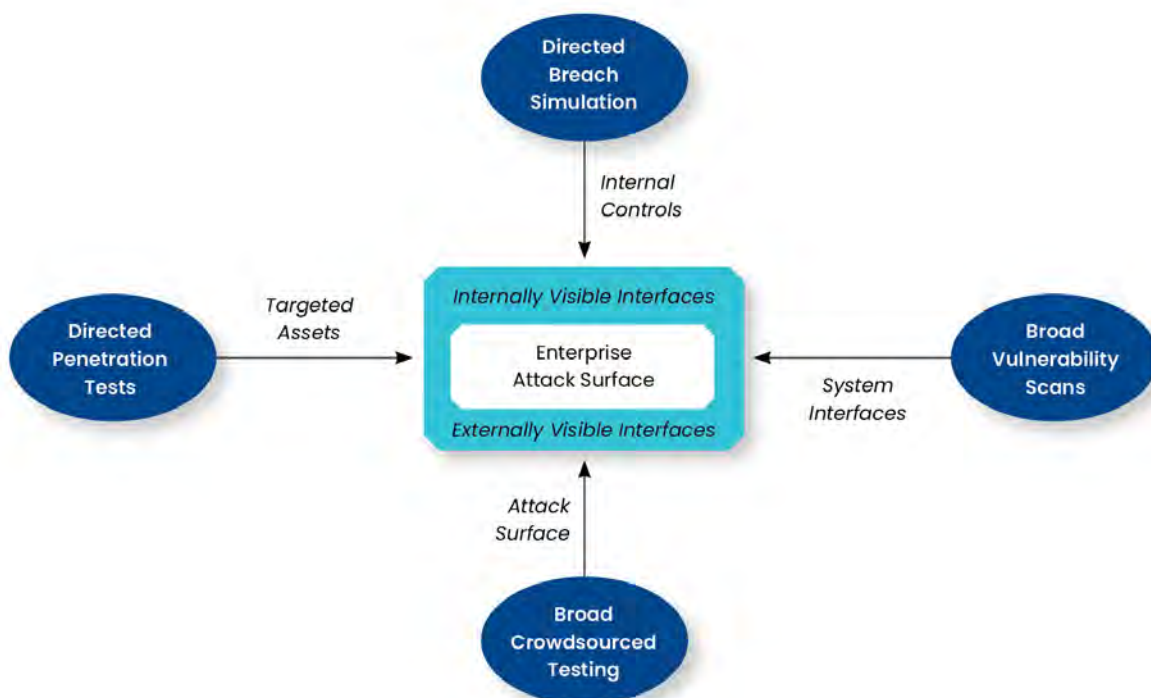


Figure 2. Common Traditional Methods for Identifying Security Posture

Case Study: Balbix Approach to Automated Security Posture

The commercial Balbix platform provides for cybersecurity posture automation. It was created to complement existing vulnerability management and related security posture capabilities deployed into the enterprise, while also addressing the major challenges and shortcomings that such functions have typically exhibited in practice for most security teams. Some teams will find that Balbix can replace their existing posture tools.

Automated Asset Discovery

The first goal of the Balbix platform is to address the ongoing challenge of inaccurate and incomplete asset inventories. Without clarity around the specific devices, apps, endpoints, and other resources in use across the enterprise, it becomes impossible to have a complete measure of security posture. This challenge is further driven by the consistent change that occurs even for those assets for which an inventory has been established.

Balbix addresses this requirement through automated, continuous monitoring of the enterprise, including traffic flows, to discover assets. The types of assets that emerge from this task include on-premises and cloud-based devices, applications, systems, and services, including managed and unmanaged assets. Fixed and mobile systems, including Internet of Things (IoT) devices are also included in the asset discovery capability.

Data is discovered in the Balbix platform using a library of connectors that can handle two primary scenarios: *streaming connector*-based collection of data in motion, and *snapshot* connector-based collection of data at rest. Both take advantage of available interfaces including data dumps and application programming interfaces (APIs) to ingest the data necessary to build accurate inventory views.

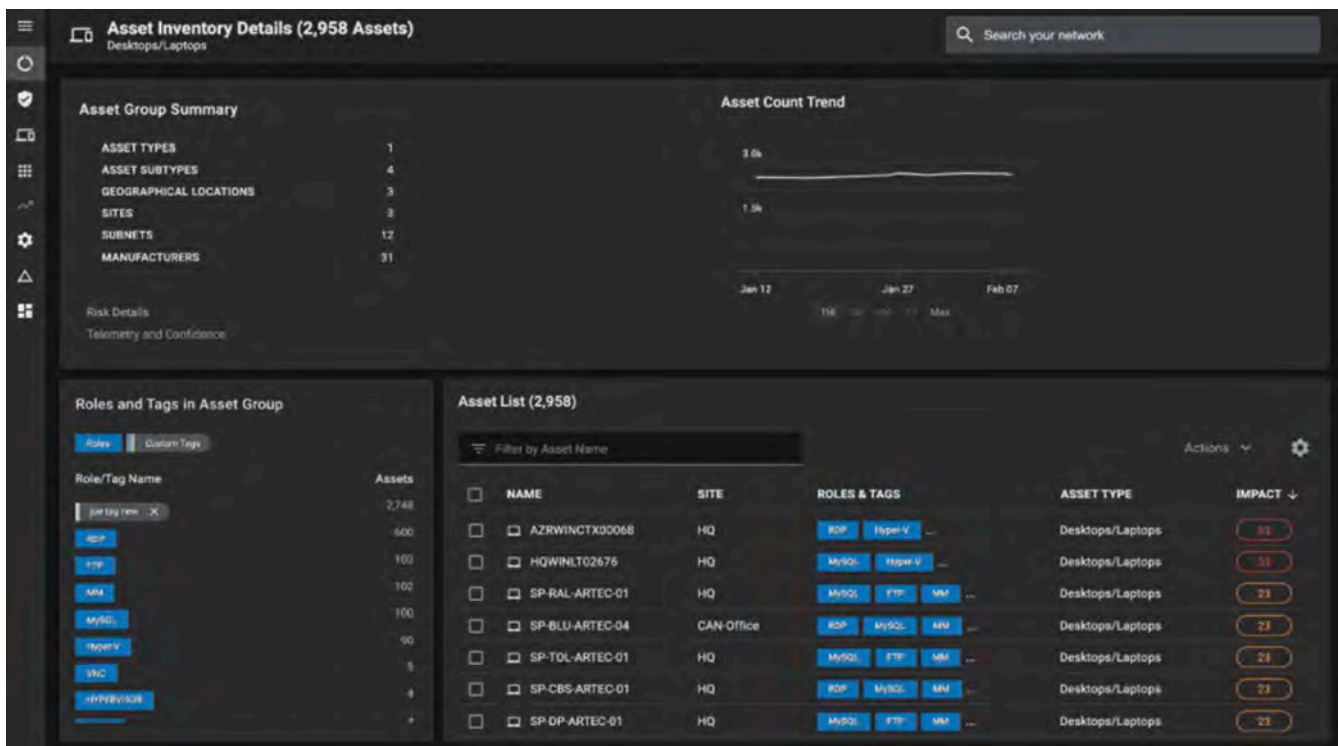


Figure 3. Balbix Platform – Discovered Asset Details

Continuous Cybersecurity Asset Management

Once a complete picture of security posture has been created for the entire attack surface, the obligation emerges to manage and maintain the asset inventory and associated context in a unified manner based on automated platform support. The Balbix platform includes support for vulnerability and risk management workflows to ensure that assets are managed continuously to provide accurate security posture even as the attack surface evolves.

The collected data is used to categorize and manage assets based on their visible attributes, including internet protocol (IP) addresses, domain name system (DNS) information, and other signals that can be used to identify entities. The technique used by Balbix to normalize the accurate asset inventory view is called *host enumeration logic*, which supports stateful, intelligent deduplication, sanitization, and other data clean-up tasks.

Such tasks must be performed at all levels of the technology stack, each of which will provide a different type of asset-related information. Layer 7 analysis, for example, will be useful to extract application-level information about assets, whereas Layer 3 and 4 analysis is useful to extract information about packet headers and protocol behaviors. The goal is to combine this collection into a unified view of the discovered asset.

Risk-Based Vulnerability Management

A major problem reported by enterprise teams is the large volume of alerts that is collected by typical vulnerability management and scanning tools. It is common for the number of alerts to become so high that security teams cannot maintain proper categorization, handling, and mitigation. This situation is ironic, because the success of vulnerability management programs is often measured based on the numbers of alerts generated.

The Balbix platform handles the volume of vulnerability management by ingesting and analyzing data from a massive number of security-related sources. These sources include vulnerability assessment tools, security scanning platforms, threat and vulnerability feeds, BAS tools, penetration testing results, crowdsourced security test output, endpoint controls, and more.

Enterprise Vulnerability Prioritization

Prioritizing vulnerabilities requires attention to relevant factors, most of which will vary in intensity between environments. The Balbix approach involves establishing five major categories of factors—severity, threat, exposure, criticality, and controls—so that enterprise teams can organize the best mitigation strategies. Such mitigation can start with those vulnerabilities that can have the greatest negative impact to critical assets.

Ultimately, the goal is to identify a breach likelihood calculation, which is a computed summation of the individual attack vector computations. Such analysis is complemented by probabilistic graph models which estimate the vulnerability levels associated with the various risk scenarios. Collectively, these computations and values provide an organization with an accurate understanding of their security posture.

Cyber Risk Quantification in Dollars

The goal of accurately establishing a quantitative measure of security posture for the organizational attack surface requires use of a risk formula that makes sense to the local domain. To avoid multiple equations, formulas, and other metrics, the Balbix platform defines a consistent cyber risk equation that can be used across all assets and over all aspects of the organization to identify a meaningful posture assessment.

The Balbix platform automates the calculation of risk in dollars. While this is certainly not a new strategy in enterprise cybersecurity, the specialized artificial intelligence models integrated into the platform support the calculation of risk trending, breach likelihood, breach impact scoring, breach likelihood by inventory, and more. These are presented in a visual display that is easy to share with both practitioners and executives.



Figure 4. Balbix Platform—Risk Quantifications

Cyber Risk Visibility and Board Reporting

The final goal of the Balbix platform is to ensure that enterprise security teams have the best available tools for reporting and explaining vulnerability and risk posture to the organization. This must include reports for senior executives including board members as well as colleagues with more detailed understanding of security programs. Such reporting must cover the entire attack surface and must account for continuing change.

Most executives will tend to focus on the impact of potential breaches, because this represents the most direct consequence of cyber risk to business operations. Balbix supports detailed impact modeling that uses impact estimates based on several factors, such as prior information, contextual impact modeling based on current usage, volumes, and interactions.

Enterprise Action Plan

It is recommended that enterprise teams act immediately to review, address, and improve their cybersecurity posture assessment. This is best done using an automated platform that can unify existing posture-related tools such as scanning and security testing. As suggested above, the Balbix platform provides excellent support in this regard and should be included in source selection plans.

¹ See <https://www.balbix.com/>.

² See <https://www.fairinstitute.org/> for information on how the FAIR (Factor Analysis of Information Risk) model supports consequence analysis based on financial impacts.

REAL-TIME MITIGATION OF CYBERTHREATS TO APIS: AN OVERVIEW OF THE SALT SECURITY PLATFORM

EDWARD AMOROSO

The protection of APIs during the entire lifecycle for software applications has emerged as an essential security requirement. This is best done through discovery of APIs, mitigation of attacks, improvement of APIs and response to incidents. The Salt Security platform is used to illustrate this critical API security control.

Introduction

The need to protect application programming interfaces (APIs) has emerged as one of the most prominent aspects of application security. In fact, the task has become so central to the protection strategies of so many organizations that it is not hyperbole to refer to API security as one of the most accelerating aspects of enterprise security, in terms of its overall impact on cyber risk.

Many strategies exist to protect APIs, ranging from MITRE ATT&CK-based testing platforms for programmers to skills development courses on how to develop and use APIs securely. The holy grail for API security, however, involves use of a platform that will discover APIs and then provide runtime security through prevention, detection and response to live threats. Such capability requires innovative technology to keep up with modern attack tactics.

In this report, we outline how this method of discovery, mitigation and response might be integrated into modern API architectures. We also show how the commercial Salt Security platform provides this type of protection for API deployments. The goal is to provide insight to enterprise security teams on how they can address this vital aspect of their overall cyber risk management program.

API Security Issues

Cybersecurity issues with modern APIs have grown considerably, as applications continue to expand in scope and usage for the typical enterprise. APIs exist for internal and external applications supporting a variety of architectures; multiple deployments, including premise, cloud and SaaS; and across many phases of lifecycle development, including the continuous steps of DevOps and CI/CD.

As a result, cybersecurity experts have had to address a range of vulnerabilities that emerge in the context of API design, deployment and use. To help, many frameworks have emerged to support the identification and mitigation of API security threats. The OWASP API Security Project, for example, maintains a top 10 list of risks to APIs that can help developers and administrators to better identify their risk.

OWASP API Security Issue	Brief Explanation
API1 Broken Object Level Authorization	Need to check authorization for every function accessing data sources.
API2 Broken Authentication	Must ensure proper authentication token usage to avoid identity threats.
API3 Excessive Data Exposure	Should always minimize views of data to only what is required for the access.
API4 Lack of Resources & Rate Limiting	Need to restrict size and number of resources being requested.
API5 Broken Function Level Authorization	Must separate authorizations for administrative and normal functions.
API6 Mass Assignment	Care is required, such as whitelisting, when binding client-provided data to models.
API7 Security Misconfiguration	Need to avoid insecure configurations such as defaults or ad hoc setups.
API8 Injection	Common issues emerge when unstructured data can be passed along to commands.
API9 Improper Assets Management	Need to track API versions and maintain accurate documentation.
API10 Insufficient Logging & Monitoring	Should provide sufficient logging to address attack persistence.

Figure 1. OWASP API Security Issues

The advantage of the OWASP API top 10 list is that it includes sensible advice from practitioners based on experiences dealing with actual vulnerabilities that have been cited in APIs. It offers a useful framework for guiding best practices in API design and implementation. The challenge, however, is that it requires diligence from developers and administrators, which can be uneven, depending on their skills and management incentives in the local environment.

Of course, it must also be acknowledged that even with diligent developers and administrators, malicious actors can abuse an API based entirely on how that interface was intended to be used. This is a general conundrum in cybersecurity, and is often best resolved through runtime detection and analysis to determine if the behavior observed matches up with what is considered an acceptable or typical use.

Real-Time Threat Mitigation for APIs

A powerful means for dealing with attacks to APIs involves the collection of live data for the purpose of detecting and mitigating actions that are indicative of malicious intent. The OWASP API list offers useful insight into the types of behaviors that might be detected in such real-time mitigation, but other actions might also be identified, using profile analysis or even machine learning models.

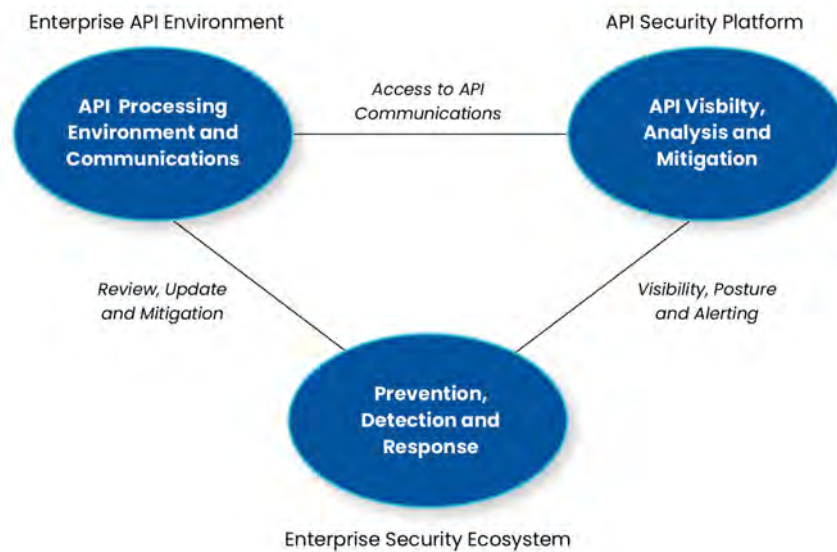


Figure 2. API Security Mitigation Approach

The mitigation of live attacks on APIs requires two preliminary steps. First, the organization must establish a means of detecting and cataloging the traffic of all applicable APIs for analysis. This collection provides the data for subsequent analysis. Second, the organization must identify any vulnerabilities that might exist in the API, through static review, API testing or other means. These steps reduce risk in advance of the dynamic coverage.

Algorithms for mitigating attacks to APIs include the familiar types of algorithmic options known to all cybersecurity experts. Certainly, signature-based solutions are possible, generally based on the OWASP list or other best practices. But since most API attacks are rooted in business logic flaws, signatures are far from sufficient—behavioral analytics must be performed to detect anomalous or unusual activity. In addition, machine learning models should be developed from training sets to detect attacks.

In the next section, we outline how one popular commercial platform from Salt Security implements these security concepts for practical enterprise API deployments. The company's commercial solution is part of a significant push in enterprise and government across all sectors to reduce API cyber risk, as more emphasis has shifted toward cooperation between applications and workloads across networks.

Overview of the Salt Security Platform

Founded in 2016 by former Israeli Defense Force members, Silicon Valley-based Salt Security provides an API protection platform that uses advanced technology to automatically and continuously identify and secure APIs. The solution is designed to complement web application firewalls (WAFs) or API gateways through use of a big data engine that utilizes machine learning to protect APIs.

Salt Security Platform Features

Several of the major functional areas supported by the Salt Security platform for enterprise security teams are outlined below.

- *API Discovery*—The Salt platform is designed to automatically discover and continuously monitor APIs of interest. The Salt system collects a copy of all API traffic, including granular data and tracking changes as the API environment evolves according to business needs. The inventory that results from this step allows for identification of shadow APIs, the APIs not released through gateways or properly documented.
- *API Data Exposure Protection*—The Salt platform reviews API data to understand the type of information being used (e.g., Social Security numbers) to flag exposure issues. This protection process also helps to identify proprietary or other sensitive data that might be shared via an API. The platform generates alerts when it detects instances of sensitive data exposure.
- *Mitigation of Live API Attacks*—The Salt platform utilizes collected API data to analyze (using AI tools), correlate and draw conclusions about possible attack conditions. The goal is to provide a means of alerting teams to live conditions or automatically mitigating live attacks as they are occurring. The platform is able to detect the reconnaissance behavior of bad actors learning the APIs, and leverages web application firewalls (WAFs) or other inline devices in the customer's environment to block the attacks before attackers can reach their objective.
- *Sharing of Remediation Insights*—The Salt platform provides insights from pre-prod and runtime environments to harden APIs. The platform performs API design analysis, comparing static OAS/ Swagger files to API security best practices, looking for gaps. It also provides attack simulation to detect business logic flaws in pre-prod. And it uses attackers as pen testers, so runtime learnings, with bad actors' minor successes, become another input for sharing remediation insights with dev teams so they write improved API design security.

In addition, the platform integrates with existing security tools and workflow systems, including Apigee, Slack, Jira, NGINX, Cloudflare, MuleSoft, Kong, F5 and AWS. It can also generate complete documentation based on the APIs and sensitive data found in runtime. These testing, integration and documentation capabilities provide useful assistance for both cybersecurity objectives based on threat and compliance obligations based on security or privacy frameworks.

Salt Security Architecture

The Salt Security architecture includes layered collection, processing, discovery and reporting. Each layer interacts with the goal of reducing API security risk based on ingested data. Positioning of the Salt platform for most environments involves a mirroring of the live API traffic via agentless collection in the API gateways, microservices, load balancers, edge processing, server and cloud infrastructure that interact via APIs with clients. The Salt platform does not deploy inline, to avoid any API performance degradation.

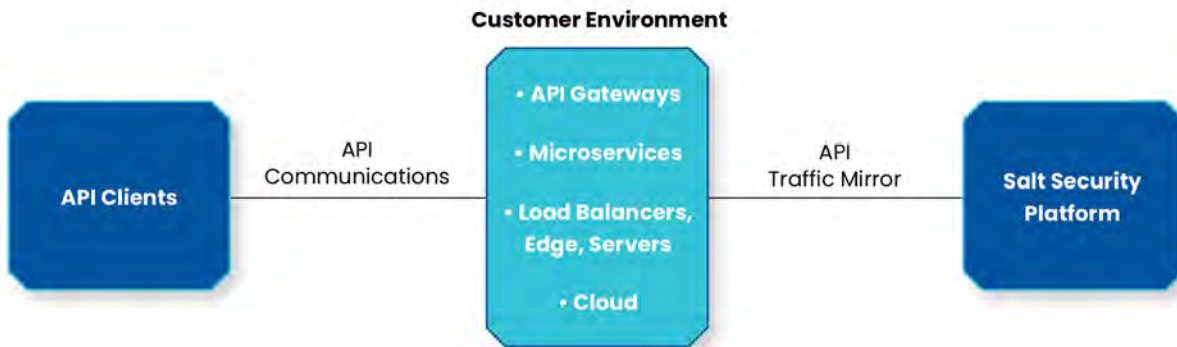


Figure 3. Salt Security Mirrored API Data Collection

Salt Security Contextual Analysis

The contextual analysis is supported by a patented API Context Engine (ACE), which takes ingested API communications traffic in mirrored form into a processing engine that utilizes machine learning to build models that can predict or detect evidence of attacks. This ACE operates at cloud scale using big data analytics, runs continuously, and can be set up to enable automated mitigation of attacks. Note that the Salt team contends that API attack detection requires cloud-scale big data—the amount of context available in an on-prem solution is insufficient to detect many of today’s sophisticated API attacks.

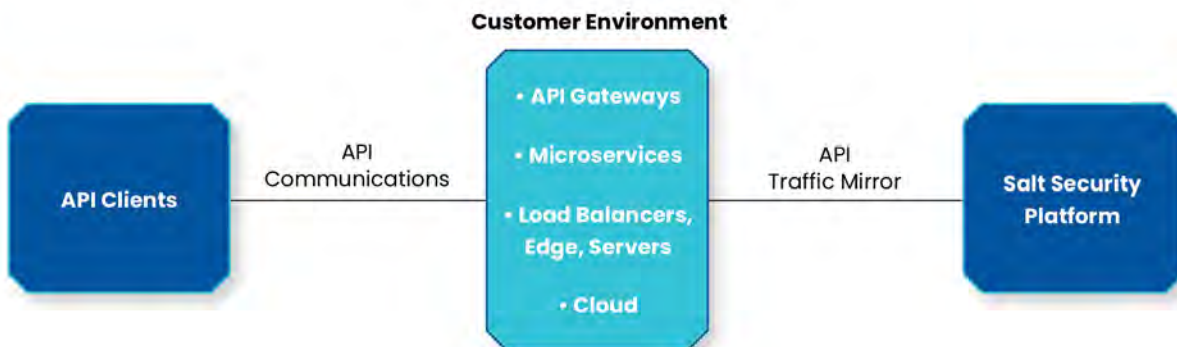


Figure 4. Processing Inbound API Traffic

The Salt Security platform can also be engaged during API development to detect vulnerabilities and gaps during build and staging and to remediate any detected issues, either in OWASP-type flaws or business logic. Runtime protections keep APIs protected regardless of when dev teams can integrate the remediation insights. The combination of shift-left and runtime protections provides the kind of full-lifecycle protections needed to provide API security for enterprise teams.

MAKING THE CASE FOR DIGITAL IDENTITY PROTECTION AS AN ENTERPRISE CONTROL

EDWARD AMOROSO

As the online threat to corporate executives and key business personnel continues to increase, especially for their enterprise organizations, the need for digital identity protection has become evident. Such protection is best done through continuous monitoring and analysis of relevant data sources for evidence of compromise. Cybersecurity start-up Sunday Security implements these controls effectively.

Introduction

Anyone with expertise in cybersecurity has experienced that awkward discussion when a family member or neighbor asks what to do after having been personally hacked. Usually this involves a password or credential being compromised, which can lead to issues with online banking or other service accounts. The bad news, which security experts are often forced to deliver, is that once personal information has been hacked, it is not easy to recover.

Some good news is that while it's not easy, recovery is possible. Perhaps even better news is that the prevention of hacks to personal digital identities can be done reliably, so long as the proper expertise is being applied. Reducing this risk is important for everyone, but is most urgent for anyone whose identity is connected to an organization. Corporate board members, for instance, must be particularly careful to avoid being personally hacked.

In this report, we explain the new types of digital identity risks that have emerged, with emphasis on the consequences of prominent business leaders becoming compromised. We also outline the best techniques for reducing this digital risk, using the emerging Sunday Security platform¹ and associated services to exemplify how these methods can be applied in a commercially available solution.

Threats to Digital Identities

Senior executives, high-profile business leaders and other key personnel have significant online digital presence. A recent study showed that in 2020, 94 percent of Fortune 500 CEOs are on LinkedIn, and 62 percent are on Facebook, YouTube or Twitter, up from 39 percent just five years earlier.² It is possible that the pandemic contributed to this increased use of public platforms, but the trend is unmistakable.

The threat that emerges is transitive: The organization is dependent on some key person; that key person has established and maintains a digital presence; and malicious actors use this presence to target the individual and, in turn, the organization. This is an important new exploitable surface that many organizations have simply not factored into their overall attack surface management (ASM) approach.

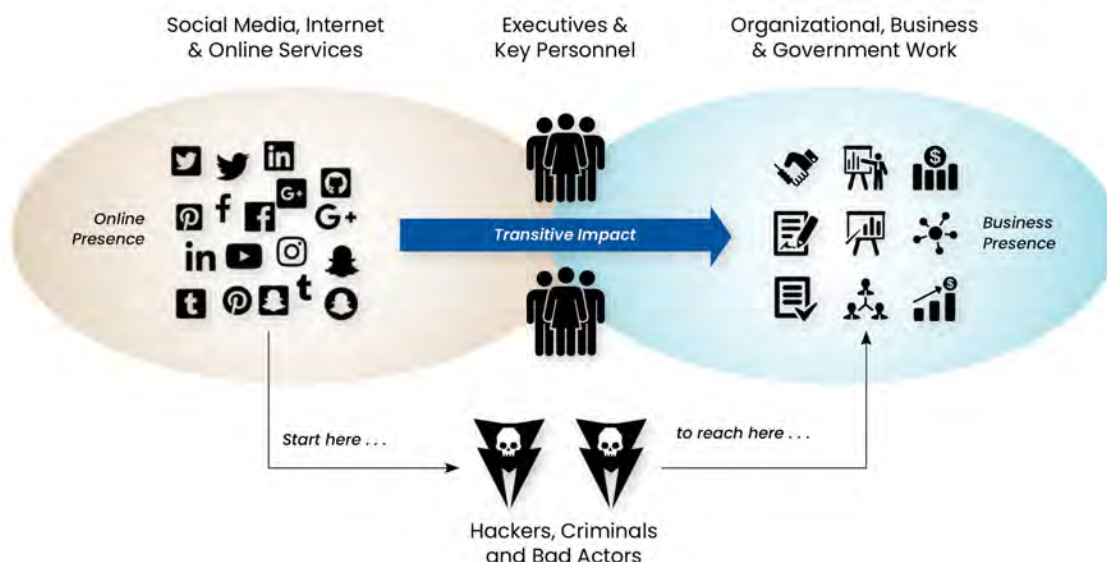


Figure 1. Transitive Attack Surface Weakness From Digital Identities

The goal therefore is to protect online accounts from being targeted for weaknesses. The power of a single account being compromised cannot be underestimated. The recent Lapsus\$ hack, for example, was executed by the hacking group using limited access from a single compromised account. This illustrates the power of offensive actors to target the single mismanaged presence of an individual.³

Cybersecurity reporter Brian Krebs said this about the group:

“LAPSUS\$ has been known to target the personal email accounts of employees at organizations they wish to hack, knowing that most employees these days use some sort of VPN to remotely access their employer’s network. In some cases, LAPSUS\$ first targeted and compromised an individual’s personal or private (non-work-related) accounts, giving them access to then look for additional credentials that could be used to gain access to corporate systems. Given that employees typically use these personal accounts or numbers as their second-factor authentication or password recovery, the group would often use this access to reset passwords and complete account recovery actions.”⁴

Nvidia took a hit from this group, with tens of thousands of its employees being leaked, resulting in “access to the source code of Nvidia’s DLSS (Deep Learning Super Sampling) AI rendering technology and information about six supposed unannounced GPUs.” A similar focus occurred in the recent Okta hack, where personal compromise was directed toward the credentials, devices and personal data of a targeted individual working for a contractor. Such activity was intended to spearhead attacks on enterprise customers.⁵

It should also be emphasized that prevention (known to security practitioners as shifting left) is a superior approach to response in the case of digital identity protection. The relatively straightforward manner in which targeted individuals can prevent most type of compromise stands in stark contrast to the difficulties that emerge when some individual’s digital presence has become hopelessly damaged.

Digital Identity Protection

Addressing the challenge of protecting online digital identities and reputations for senior executives and key personnel should be viewed as a risk management problem. That is, rather than expect to close off any personalized vulnerabilities that might emerge for business leaders in their external profiles, a more reasonable view is that effective methods can be deployed to manage and contain the risk.

Solutions to digital identity protection for an organization will fall into three major categories. First, there might be an awareness program to help executives and key personnel better manage their online personas. This is a good idea, regardless of whether additional controls are being deployed. Organizations would thus be wise to ensure that good information is being made available to employees about safe and secure online behavior and social media usage.

Second, there might be policies and practices to limit the degree to which employee use of social media and other online services can reference, use, link to or otherwise connect to organizational assets. Some organizations, for example, do not permit access to social media from company-issued devices. Both this approach and the awareness case will not increase risk, but are certainly not strong, dependable controls.

The third and strongest case involves a security solution that uses a technology-based platform to reduce risk. Specific functional features that enterprise security teams should demand in any technology-based platform include the following features:

- *Continuous Coverage*—The technology platform should include the capability to automate the collection and processing of data to provide ongoing and continuous visibility into personal and enterprise digital risks.
- *SaaS Support*—When implemented as an online SaaS solution, the platform should be easily accessed from the variety of different personas and contexts associated with digital identity risk.
- *Advanced Analytics*—Technology-based solutions should include a means to correlate information and perform advanced processing, using profiling or machine learning to detect or even predict risky situations.

When implemented correctly, the platform will employ these attributes to ensure proper levels of security and to serve as a foundational base for all types of digital identity protection. Commercial implementations are beginning to appear (see section below), so security teams will have good options to address this risk in a more continuous and effective manner.

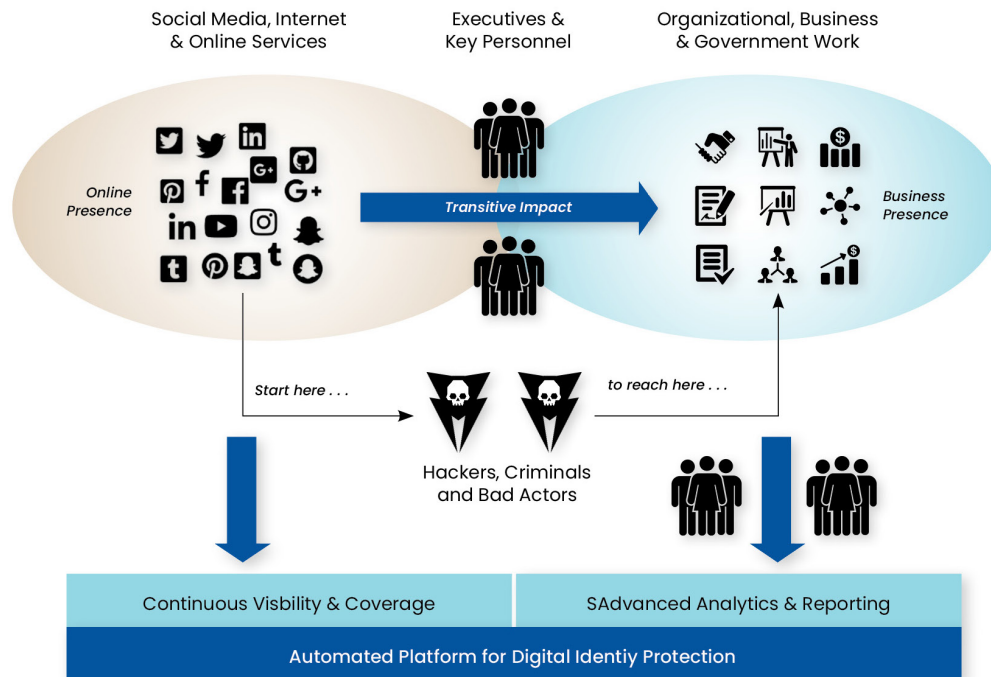


Figure 2. Using a Technology Platform to Reduce Digital Identity Risk

The next section includes a description of a new commercially available SaaS platform being developed at cybersecurity start-up Sunday Security, with the goal of implementing exactly the types of functional controls described above.

Overview of Sunday Security

Founded in 2021 by Tsachi Ganot and Shaked Barkan, Sunday Security focuses on securing the digital identities of prominent individuals such as senior executives, key business leaders and other high-profile personnel. The company has assembled an impressive advisory and investor board, which includes many individuals with exactly the type of prominent profiles that are expected in customers of the Sunday Security solution.

The primary goals of the Sunday Security solution, which is currently emerging onto the marketplace for commercial use, include the following:

- *Executives and Key Personnel*—The Sunday Security solution is designed to address risks to executives and key personnel, using the targeted approaches described above. The goal is to ensure that organizations reduce their risk by addressing the digital identities of their people.
- *SaaS Platform Solution*—The Sunday Security solution is provided through a SaaS-based platform with the ability to plug into enterprise security platforms for rapid and accurate notification and response.
- *Advanced Algorithms*—The Sunday Security solution works from a vector of applicable factors related to digital identity risk and uses advanced processing techniques to draw conclusions about risk and to provide guidance for effective actions to avoid the consequences of a compromise.

¹ The company is also known as Pandora Security.

² <https://influentialexecutive.com/how-many-fortune-500-ceos-social-media-2020/#:~:text=We%20manually%20combed%20through%20this,least%20one%20social%20media%20platform>

³ <https://www.theverge.com/2022/3/22/22991409/lapsus-microsoft-security-windows-source-code>

⁴ <https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/>

⁵ <https://www.analyticsinsight.net/lapsus-a-prolific-hacking-gang-targeting-the-high-profile-companies/>



**DISTINGUISHED
VENDORS**

DISTINGUISHED VENDORS

Q 3 2 0 2 2

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

ANOMALI

Anchored by big data management, The Anomali Platform, an Open XDR solution, drives detection, prioritization, and analysis to stop breaches and attackers in real-time. By fusing threat intelligence with precision detection capabilities, Anomali enhances threat visibility, automates detection, and accelerates threat investigation and response. The product suite includes ThreatStream®, Match™, and Lens™.

Acronis

Acronis integrates data protection, cybersecurity and endpoint management as a centralized, seamless all-in-one cyberdefense that unifies protection of entire data, applications and systems. Its AI-based behavioral detection engine stops malware, ransomware, cryptojacking and zero-day attacks. Advanced packets offer automated disaster recovery and enhanced protection for email, backup and cloud security.



Arctic Security

Using external cybersecurity monitoring, Arctic Security offers an Early Warning Service that provides information about all threats in a company's network. To prevent issues before they happen, automation tools—Arctic Node and Arctic Hub—effectively collect threat intelligence in order to identify vulnerabilities and any early signs of security breaches.

BLACKCLOAK™

BlackCloak extends enterprise security by protecting the personal digital lives of executives, Board Members, and high-access employees, and their families, from targeted cyberattacks and fraud. Their digital executive protection platform combines online privacy protection, personal device and home network security, and incident response, with a US-based SOC and concierge service.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 2



Cider offers effective application security for engineering ecosystems. Ready-to-use integrations take seconds to deploy and address all requirements for releasing secure software at scale. Provided is support for all technologies—from code to deployment—as well as comprehensive, accurate analysis of frameworks and assimilations that exist in the CI/CD environment.



With offices around the world, Constella Intelligence provides Digital Risk Protection Solutions that are collaborative and expansive. Services offered include all-encompassing threat detection software, identity monitoring of both surface and deep/dark webs, cyber risk intelligence defenses and thorough cyber investigation that unmask threat actors and detects hijacked and fake accounts.



ControlCase provides continuous compliance service solutions to address all aspects of IT governance, risk management and compliance management. As an ASV and QSA of PCI DSS, ControlCase, with its international staff of professional auditors, offers clients comprehensive solutions to meet objectives set forth in all federal legislation governing financial institutions.



Corelight supplies pioneering network detection and response technology to help defend sensitive, mission-critical organizations. With its enterprise-ready Zeek® and open access NDR platforms, Corelight's evidence-centric approach transforms network traffic into coherent and tangible data—easily customized and accessed—that allows companies to expand their visibility, reduce risk and improve productivity.



Cyber Security Solutions offers clients full protection and peace of mind with their all-in-one security solution, full compliance dashboard, secure file management system, 24/7 monitoring, industry certified practices and a personal onboarding process. Turnkey cyber solutions protect a variety of industries from insurance to law enforcement; medical to regulatory compliance.



Cymulate's Extended Security Posture Management allows organizations to measure and maximize operational efficiency while minimizing risk exposure. Based on real-time data, Cymulate protects IT environments, cloud initiatives and critical data against threat evolutions. Using simulation, evaluation and remediation, Cymulate empowers and defends organizations worldwide, including leading healthcare and financial services.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 2



Cynamics guarantees unified network threat detection, providing a new cybersecurity paradigm. Combining AI and deep learning to analyze patterns and autonomously identify malicious behavior, Cynamics predicts threats long before they hit. Their patented AI technology—Novel Threat Detection—delivers 100% network coverage 24/7, reducing costs and complexities while removing onboarding roadblocks.



Cyvatar offers automated and fully managed cybersecurity services for startups and small to medium-sized enterprises. Based on industry-recognized CIS 20 Critical Controls, Cyvatar's Outcome Platform accelerates the traditional install, configure and assess methodology, allowing companies to analyze, contextualize and translate complex technical data quickly and seamlessly to reach effective remediation.



Garrison's web isolation solutions deliver security for strategic digital transformation. Through the development of the world's first hardsec cloud, Garrison powers enterprise-wide secure web-access, protecting users from phishing attacks and internet-borne malware. Applying technology advanced by the National Security sector, Garrison builds flexible and scalable IT for the commercial world.



Integrating seamlessly with any SDLC, GitGuardian's code security platform scans, detects and remediates, bringing developers, security teams and cloud operations together. Using hundreds of automated, fixed sensors that scan thousands of git repositories, GitGuardian's detection engine provides companies with customized detector technology to reduce the risk of secret data exposure.



IGI CyberLabs' innovative Nodeware® software combines new device recognition with vulnerability scanning to improve network security with powerful exposure management and visibility. Nodeware® allows businesses to monitor their network, identify security gaps and access detailed reports with an easy-to-use interface to achieve security compliance and protect networks from any cyberattacks.



Laminar offers the first extensive cloud data security platform for everything built and run in AWS, Azure, GCP and Snowflake. The platform helps security and governance teams autonomously discover, prioritize and secure their data with continuous monitoring. Data is embedded into the cloud infrastructure, ensuring optimum defense against security breaches.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 2

noetic

Noetic offers an intuitive, proactive approach to cybersecurity with its continuous, automated cyber asset management and controls platform.

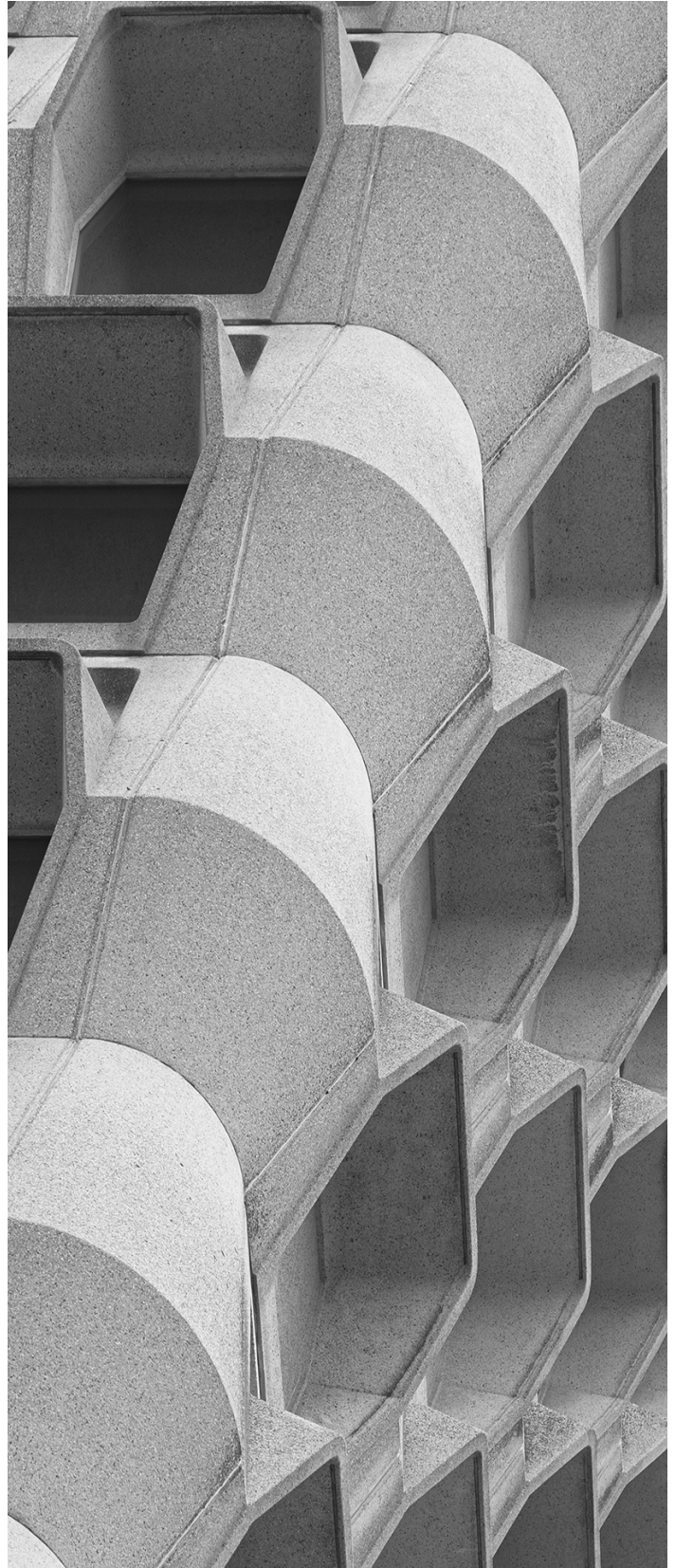
Dashboards identify and prioritize significant security insights across endpoints, users and cloud systems. This team of security industry veterans is enabling enterprises to prioritize their efforts on reducing risk on the most critical systems in their cyber environment.

n noname

With its API Security Platform, Noname Security protects APIs by identifying security risks and proactively detecting vulnerabilities, misconfigurations and design flaws before they can be exploited. While providing automatic detection and response and automatic blocking and threat remediation, the platform connects to any environment and integrates easily with existing technology.

Prevalent™

The Prevalent Third-Party Risk Management Platform is a complete solution that unifies vendor management, risk management and threat monitoring. The platform makes it easy to onboard and assess vendors; correlate those assessments with external threat data; reveal, prioritize and report on said risk; and facilitate any necessary remediation processes.



TAG CYBER DISTINGUISHED VENDORS

2 0 2 2

PREVAILION

Prevailion is a cyber intelligence company that protects organizations by providing unmatched insights into real-time threats targeting their networks. Offering clients the Apex™ Platform that predicts pre-attacks, detects early stage infiltration and provides total supply chain visibility, Prevailion collects malicious communications originating from threats that have bypassed existing security controls.



Q-NEXT mitigates the risk of ransomware crises by offering a proprietary Zero Trust Data Access platform called FileFlex Enterprise. Built with its patented technology, FileFlex Enterprise is an overlay solution that enables any major sector organization, from healthcare, financial, to public transportation, to unify remote access, sharing, and governance of unstructured data storage across entire Hybrid-IT and Multi-Cloud infrastructures.

REVERSINGLABS

ReversingLabs unifies software development and security operations teams with its Titanium Hybrid-Cloud Platform for software supply chain security protection. The platform reduces attack surface risk by utilizing extensive intelligence monitoring to harvest thousands of file types at scale through deep software and file threat analysis, accelerating data release and response.



The Rezilion platform offers detailed, autonomous cybersecurity solutions powered by its analysis engine Unison™. Deployed in seconds as a plug-in to existing DevOps tools, Unison™ reverse-engineers and maps an entire environment, tracking inventory, provenance, runtime execution, exposure and interdependencies within each piece of code to prevent risk, drift and delays.



RiskIQ maps threat intelligence on a global scale through multiple automated discovery and continuous scanning platforms that secure an enterprise's attack surface. Composed of former NSA and intelligence officers, the RiskIQ Service team delivers precision-focused monitoring of a company's digital security, mitigating exposure by fingerprinting, detecting and thwarting cyber risk.



With its breach and attack simulation platform, SafeBreach provides a hacker's view of a company's ecosystem to help security teams switch from defense to offense. Simple to deploy and integrate, the SafeBreach platform proactively maximizes impacts of security controls: identifying and prioritizing threats, revealing vulnerabilities and improving cloud security posture.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 2



SailPoint is the leading provider of identity security for the modern enterprise, empowering organizations worldwide to put identity security at the core of their business. With a foundation of artificial intelligence and machine learning, SailPoint identity security delivers the right access to the right identities and resources at the right time.



Salt Security, with its patented API Context Engine Architecture, offers clients complete API security with the ability to stop every API attack and eliminate API vulnerabilities. The platform collects API traffic across an entire application landscape, using AI/ML and its cloud-scale data engine to reveal exposed data and enable remediation.



The Sertainty Data Privacy Platform provides unparalleled security risk mitigation. By embedding an Intelligent Module directly into data itself, Sertainty does away with unsustainable, indirect approaches to data privacy. Private information becomes tamper-resistant; self-tracking and authentication cover life cycles of digital assets, from copyright protection to registration and royalty administration.



Sevco Security offers persistent cybersecurity situational awareness for all corporate IT and Security Operations Teams. Comprised of cybersecurity leaders from top commercial vendors and U.S. Intelligence, Sevco Security is dedicated to giving enterprises all that's needed to ensure they know what everyone on-premise and off is doing at all times.



ShardSecure desensitizes sensitive data in multi-cloud, hybrid-cloud and private cloud environments while reducing management complexity and improving business continuity. Headquartered in NY with its engineering team in Sweden, ShardSecure offers innovative Microshard™ Technology that protects sensitive resources in the cloud by securing and preserving data backup and preventing file tampering.



Sicura is an automated security and compliance platform that seamlessly enforces and remediates technical security controls, fixes misconfigurations, and prevents security drift. The Sicura team of NSA veterans has built a product that bridges the gap between security and engineering teams, driving efficiency and improving enterprise security posture.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 2



Sonrai Security offers total cloud security in one platform that unearths, prioritizes and removes risks across every part of the cloud. Their proprietary, big data analytics engine continuously updates the paths an identity has used or could use to access data, and offers visibility rooted in full context and actionable understanding.



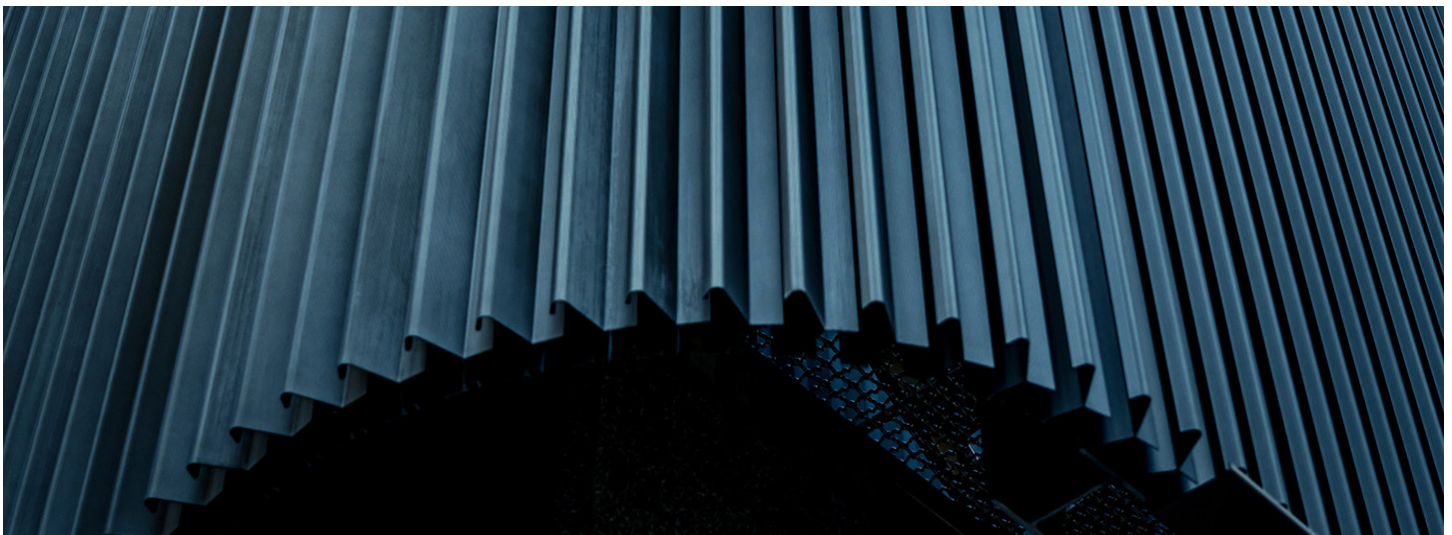
Sunday Security is a digital executive protection program, built to protect the world's executive teams beyond the enterprise perimeter. By harnessing our proprietary personal security platform coupled with our personal SOC, Sunday provides enterprise-grade personal cybersecurity to those at the enterprise who need it most.



Titanium's advanced Data Security Platform utilizes encryption-in-use to make an enterprise's data immune to compromise without loss of functionality. The platform offers automatic compliance, flexible architecture, third party data control and fast, easy deployment. When all other security controls are breached, Titanium continues to defend against ransomware and other cyberattacks.



TrueFort offers application focused security at Wall Street speed and scale. Its award-winning fortress platform security system consolidates multiple fragmented security tools—cloud detection and response, zero trust segmentation, service account analytics, workload hardening and file integrity monitoring—to seamlessly shut down all unusual behavior and prevent malicious cyber infiltration.





TAGCYBER

© 2022