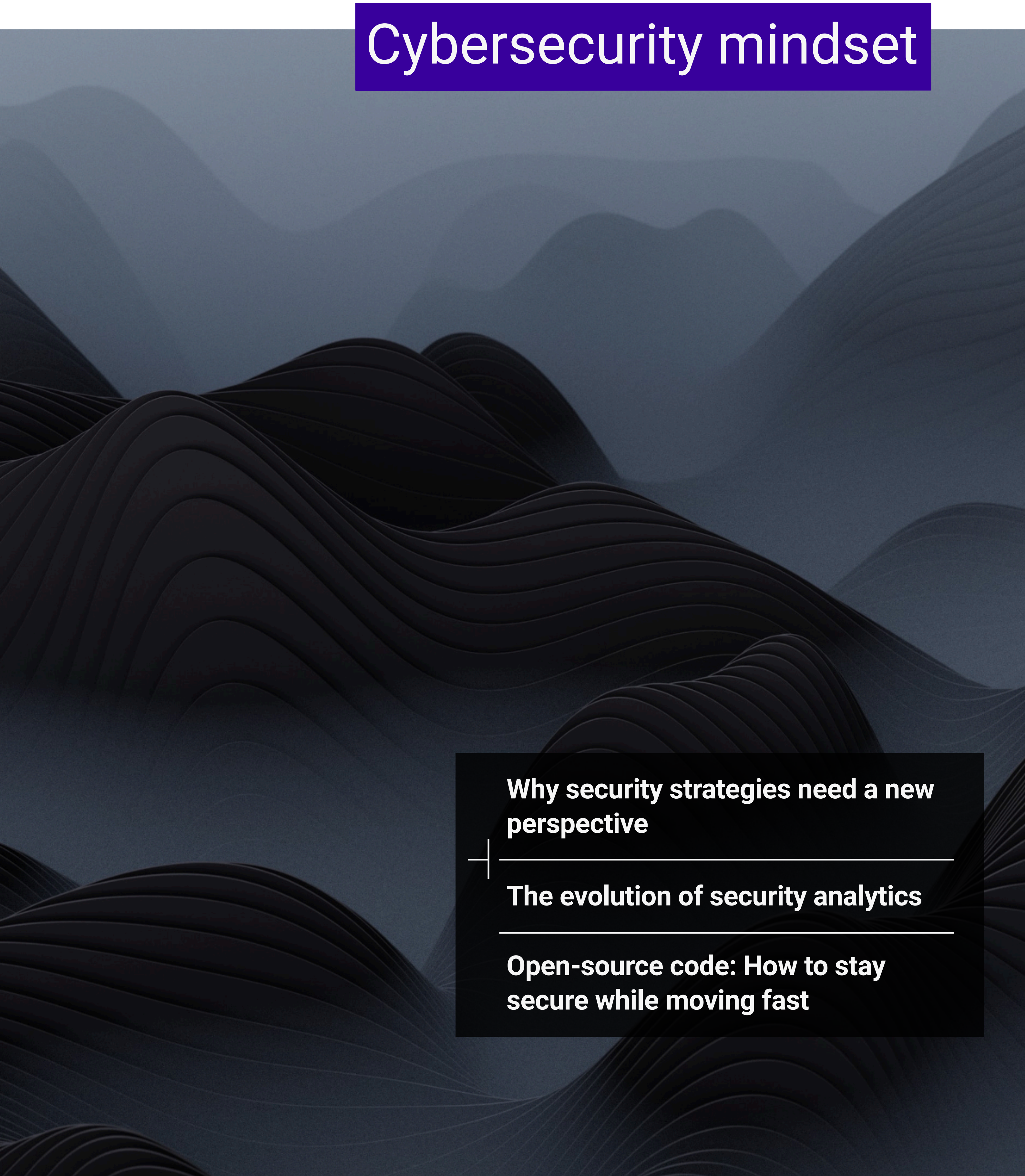
[+] (IN)SECUREMagazine

03 | 2022

ISSUE 71

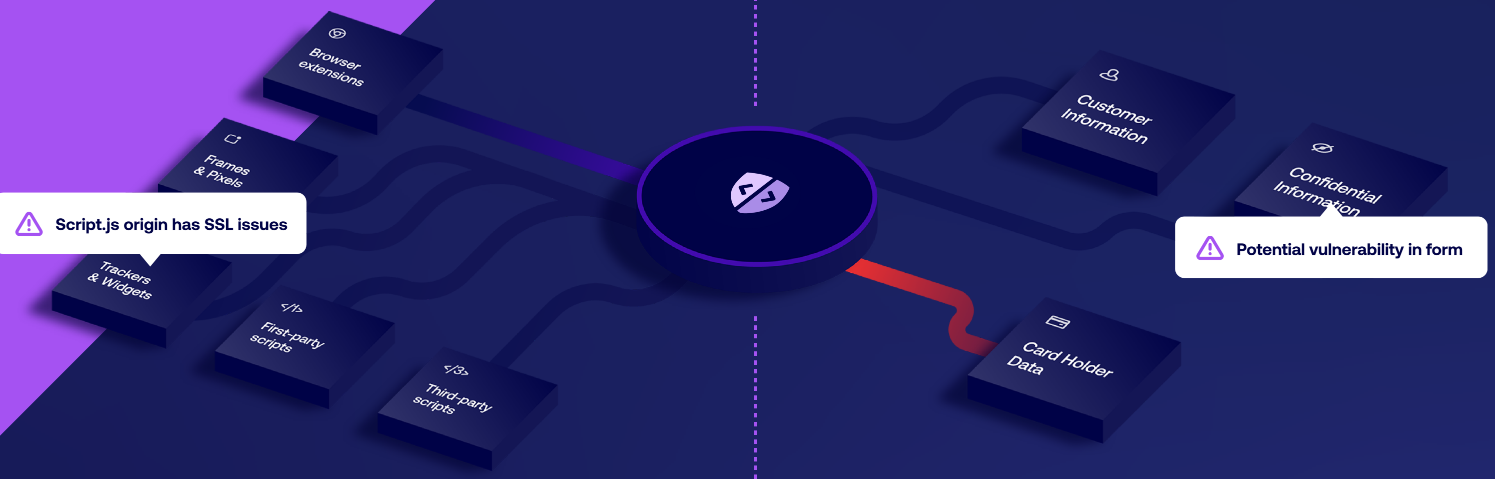
Cybersecurity mindset



Why security strategies need a new perspective

The evolution of security analytics

Open-source code: How to stay secure while moving fast



Client-side Security

Yeah, We Fix That

- Prevent client-side security threats
- Know your client-side attack surface
- Uncover suspicious behavior
- Act on privacy & compliance reports

Secure your JavaScript with automated security scanning, monitoring, and controls.

feroot

See it in action at **feroot.com**

Table of contents

Featured experts

SEAN ARROWSMITH, Director, Crossword Cybersecurity
BENJAMIN ANDERSON, CTO, Cloud, EDB
ONKAR BIRK, CTO, Alert Logic
TIM CALLAN, Chief Compliance Officer, Sectigo
TONY COLE, CTO, Attivo Networks
DARREN FIELDS, VP of Cloud Networking EMEA, Citrix
GUY GILAM, Head of Product Marketing, Cybellum
RYAN LLOYD, Chief Product Officer, Guardsquare

JOHN MILBURN, CEO, Clear Skye
SARYU NAYYAR, CEO, Gurucul
MARTIN REHAK, CEO, Resistant AI
LARKIN RYDER, Director, Product Security, Slack
BEN SMITH, Field CTO, NetWitness
MATT TESAURO, Director of Security Evangelism, Noname Security
RIZWAN VIRANI, President, Alliant Cybersecurity

Visit the magazine website and subscribe at www.insecuremag.com

Mirko Zorz
Editor in Chief
press@helpnetsecurity.com

Zeljka Zorz
Managing Editor
press@helpnetsecurity.com

Berislav Kucan
Director of Marketing
bkucan@helpnetsecurity.com

Distribution of modified versions of (IN)SECURE Magazine is prohibited without permission.

Five tips on how to stay (cyber)secure in a hybrid work world

Larkin Ryder

Director, Product Security, Slack

From less time spent on the commute to a better work-life balance, maintaining the newly discovered possibilities of flexible working is a firm priority for workers today.

For businesses, that means hybrid work is here to stay. Not only does it help create a more attractive workplace at a time when job vacancies have been hitting record highs, but ultimately hybrid flexibility can drive greater engagement, better satisfied teams, and more productive businesses.

However, in the rush to embrace this new world of work, it's been all too easy to overlook one of the biggest challenges it creates: maintaining cybersecurity.

Bad actors have taken advantage of uncertainty and change in the past eighteen months to exploit businesses and their workers. By following a few tips, though, we can stop them in their tracks, and unlock the benefits of a hybrid future of work without sacrificing security.

Tip one: Recognise your risks

Online fraud rose by 70% during the pandemic as bad actors took advantage of increased home working and reliance on online devices. From COVID-19 testing scams to launching hacks through QR codes, the first step to boosting security is recognizing the different shapes and sizes security risks come in.

Security leaders must continuously make the time to identify new threats and vulnerabilities and plan for improved detective and preventive controls, to ensure their business stays ahead of those risks.

> *Online fraud rose by 70% during the pandemic as bad actors took advantage of increased home working and reliance on online devices.*

On top of this, it's also worth understanding the implications of weaker security, and educating the wider business on this topic. Not only can it impact the business' bottom-line, but research suggests victims are also hurt emotionally, with lower levels of happiness and higher levels of anxiety. Security today isn't only about protecting your technology and finances, but also your people.

> *As you're heightening your people's awareness of security risks, remember to lead with empathy.*

As you're heightening your people's awareness of security risks, remember to lead with empathy. Communicate that the security team is ready to help and support whenever people have security concerns.

Tip two: Reduce reliance on email

Email is the leading attack vector used by attackers to gain access to businesses and their employees. One of the most common approaches is through email spoofing, in which a bad actor creates an email that appears to be someone else (often, someone senior at the business they are targeting).

For both internal and external communication, changing email habits and reducing reliance upon it is now simpler than ever. This can be one of the most effective ways to reduce exposure to attacks and fraudsters. And, on top of this, bringing communications out of siloed email chains and into a tool like a channel-based messaging app has the benefit of making those communications not only more secure, but easier to share with team mates to collaborate on.

Tip three: Empower your employees with enterprise-grade tools

IT teams must stay ahead of employee needs. Otherwise, employees will find a solution to fill their needs, increasing the risk of disclosure of sensitive information. And, once adopted, it's hard for companies to unwind this so-called "shadow IT." In short, leaving teams to informally fill gaps in their tech suite - for example, by using consumer-grade messaging apps to communicate - creates unnecessary security risks.

Encryption is a bare minimum for workplace collaboration, however enterprise-grade apps can provide additional features like Enterprise Key Management, audit logs which further empower IT teams to keep data secure and workers safe.

> *IT teams must stay ahead of employee needs. Otherwise, employees will find a solution to fill their needs, increasing the risk of disclosure of sensitive information.*

Further, having a dedicated security and compliance partner ecosystem means enterprise-ready collaboration tools can easily connect with security staples (e.g., Okta or Splunk).

Tip four: Boost identity and device management controls

With more workers using personal Wi-Fi and personal devices it's time to establish new security baselines. Securing information in a hybrid working environment begins with identity controls.

From session duration metrics to two-factor authentication and domain claiming, it's crucial to think twice about how you're ensuring only the right people have access to your company's information, wherever they're working.

Meanwhile, session management tools, default browser controls, additional authentication layers and the ability to block jailbroken or rooted devices are extra defenses that help ensure that it's not just approved people, but approved devices that are plugging into your networks.

Tip five: Embrace a mindset shift on security

Just as the work landscape has changed dramatically since early 2020, so has the security space. As workers shifted, so did threats, and IT teams have worked tirelessly to stay ahead of fast-moving bad actors.

We know remote work is here to stay. Meanwhile, new threats such as weaponized artificial intelligence are only just emerging. To help IT teams do their job and keep us and our businesses safe, we must start shifting our mindset on security.

That means formalizing the work-from-home space and enabling workers and IT teams to give it the same level of protection as we'd expect in a physical office. It also means listening to the needs of remote and hybrid workers and providing everyone with enterprise-grade tools for work, from office suites to collaboration tools, so that they never have to turn to non-enterprise grade or unsanctioned platforms.

> *We know remote work is here to stay. Meanwhile, new threats such as weaponized artificial intelligence are only just emerging.*

Finally, it means always taking a security-first approach to the tech-stack. Reducing reliance on legacy tools that provide bad actors with exploitable gaps in your defense and building an ecosystem of enterprise-grade tools can enable businesses to shore-up security. The result is IT teams and the organization as a whole can work from anywhere, and focus on the work that really matters to them, safely and securely.

> *Reducing reliance on legacy tools that provide bad actors with exploitable gaps in your defense and building an ecosystem of enterprise-grade tools can enable businesses to shore-up security.*

Open-source code: How to stay secure while moving fast

Benjamin Anderson

CTO, Cloud, EDB

Open source has transformed the software world, tremendously reducing the cost of introducing new technology by enabling broad reuse across products and industries. However, organizations pulling their code from open source will often find themselves in scenarios where they have created a Frankensteined final artifact, with extremely fragmented origins.

This can cause problems when organizations fail to consider long-term support of the open-source libraries they rely on, and at worst can create security problems within their applications. The series of Log4j vulnerabilities in late 2021 is a perfect example of this. Organizations must take time to carefully consider their approach to supply chain security to prepare for potential future security incidents, and to gain the full benefits of open source.

Open source isn't exactly free

Code derived from multiple sources brings unique security challenges that organizations are not always equipped to handle - or even aware of. The supply chain can be incredibly complex, composed of a massive tree of open-source dependencies, all being updated on a regular basis. IT teams do not typically audit every line of code in their system when upstream open-source software is updated or changed. With a web of dependencies, constant changes, and lack of deep evaluations from IT teams, external security threats should be very much a concern, despite the origins from outside the organization.

> *Code derived from multiple sources brings unique security challenges that organizations are not always equipped to handle - or even aware of.*

Regardless of who is initially responsible for the bugs, organizations face liability when shipping software that includes vulnerability-ridden open-source code. Without processes in place to vet open-source inclusion and updates, organizations will continue to fall into the trap of utilizing open-source components without understanding the risks they are undertaking. Furthermore, as the software world continues to evolve, new technologies such as containerization will put a secure posture even further out of reach.

Upon publication of a vulnerability in an open-source project, organizations can be crushed with the burden of auditing updates to all relevant software updates within potentially tight deadlines. This can devastate developers' productivity, as subject matter experts must choose to either audit thousands of lines of code, blindly accept the latest version of their dependencies, or both, risking introducing bugs in the process.

> *Upon publication of a vulnerability in an open-source project, organizations can be crushed with the burden of auditing updates to all relevant software updates within potentially tight deadlines.*

Despite the risk factors, there are ways for organizations to effectively secure and protect their usage of open-source code. With greater understanding of dependencies, and proper checks-and-balances in place to mitigate risks, teams can begin to feel secure in their open-source utilization and fully embrace its benefits.

Difference-makers to keeping open source secure

IT leaders should first and foremost establish policies that focus on threat and risk mitigation prior to beginning projects. Policies ensuring review and approval of new open-source dependencies, as well as regular updates of those dependencies are a must to reduce the risk of future disaster scenarios. This must be done with buy-in from development, of course – developers want to use the latest and greatest tech, and if they can't use the best tool for the job they won't be happy developers – but a minimal baseline policy can help frame the problem.

Inventory and regular maintenance are key here because you can't fix what you're not aware of, and it's vastly easier to update a dependency from last week's release than it is to update from a release from the last decade.

Once these guidelines are in place, development should take the lead in implementing procedures to meet the policy requirements. This is where DevSecOps comes in: bringing a software development mindset to solving security problems can reduce cost and help break down barriers within organizations.

Firstly, teams need to understand what software is deployed in their environments, assuming they haven't been documenting a bill-of-materials from the outset. This can be difficult because there are many layers of dependencies in a modern software stack.

For one example, most container vulnerability scanners are limited to packages installed via the operating system package manager (e.g., apt or yum). By design, this misses many dependencies such as statically linked binaries, manually installed packages, programming language dependencies, and more.

Secondly, teams need to implement processes for keeping dependencies up to date. While this can be a strain on developer time and resources, this ongoing cost is assuredly much less than what would be required of teams during an unexpected breach - and more financially secure, as well.

Alternatively, organizations that do not have the developer resources to inventory dependencies and continuously monitor for vulnerabilities should reduce their security footprint by using platform-as-a-service (PaaS) products from cloud service providers. For example, purchasing a database-as-a-service (DBaaS) product rather than self-hosting a PostgreSQL cluster on a set of virtual machines can eliminate an organization's responsibility for a very large stack of dependencies. This can allow teams to shift the focus away from mundane "undifferentiated heavy lifting" and toward innovation and business value.

Pulling the good out of the box and sealing away the bad

Organizations can - and should - take advantage of the rich rewards of the open-source community for excellent code and innovative solutions. But this must come with consideration and planning for the potential security risks at hand.

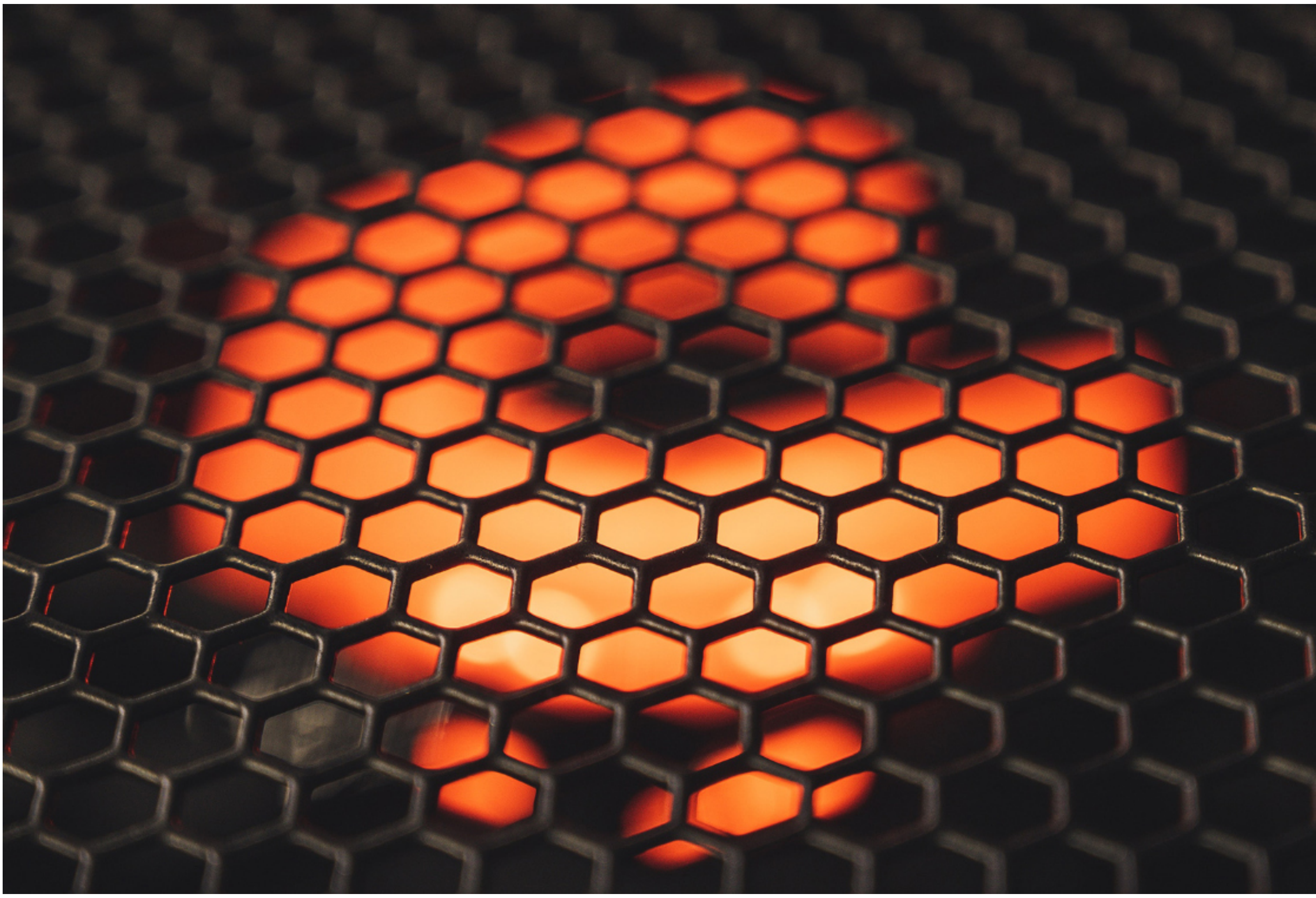
IT leadership teams can significantly mitigate supply chain risk when they take appropriate steps to evaluate and guide inclusion of open-source dependencies. Preparing ahead of time can give peace of mind today, keep the risks at bay, and encourage developer innovation.

PRODUCT SHOWCASE

Learn more about the latest information security solutions

HELPNETSECURITY

helpnetsecurity.com



Enterprise PKI automation: The modern approach to certificate lifecycle

Tim Callan

Chief Compliance Officer, Sectigo

Today's modern enterprises face massive surges in the use of digital identities, both for machines, (servers, laptops and network devices) and for the humans who use them. In the wake of this identity explosion, it has never been more important for IT teams to govern, authenticate and secure every single digital identity in the organization - without exception. The challenge faced by already strained IT teams is how to deliver strong certificate management across increasingly complex IT environments, at a time when workforces are massively distributed and entering the corporate network via the consumer-grade technologies in their homes.

As enterprises rush to combat these issues, digital certificates based on public key infrastructure (PKI) are an increasingly trusted way for enterprises to authenticate identity. The digital identities provided by PKI collectively yield one of the strongest, easiest-to-use authentication and encryption solutions available.

> *The digital identities provided by PKI collectively yield one of the strongest, easiest-to-use authentication and encryption solutions available.*

Enterprises have different options for obtaining and managing digital certificates. While third-party certificate authorities (CAs) are a trusted option for many enterprises across the globe, many choose instead to issue them in-house, operating their own "private CAs" to fulfill at least a portion of their PKI needs. The general idea in doing so is to maximize control over the authentication process.

To fully realize the benefits of a private CA, IT leaders require a solution that:

- Covers all types of certificates deployed across the enterprise.

- Supports an architecture with any combination of root CA and issuing CA, from private and third-party authorities.

- Supports the entire certificate lifecycle management (CLM) process, enabling issuance, deployment, renewal, and replacement of certificates quickly, reliably, and at scale.

Manual PKI management is risky and costly

Meeting all these requirements is not always straightforward, as private CAs involve additional drawbacks such as higher risks and higher costs and require hands-on complex management. Many organizations still manually manage their certificates using tools like spreadsheets to track the lifecycle of each individual certificate. Perhaps the most significant risk of manual certificate management is the inevitability of human error. Given time, humans will make mistakes; in the case of certificate management, a single mistake can result in serious consequences.

> *Many organizations still manually manage their certificates using tools like spreadsheets to track the lifecycle of each individual certificate.*

An expired certificate, which is very common with manual PKI management, will certainly cause problems. The best-case scenario is a service outage emerging from legitimate transactions that simply fail. The worst-case scenario involves staggering damage to the organization's global public reputation and brand, resulting in millions of disgruntled end-users. That's what happened to Ericsson in 2018 when a single expired certificate left tens of millions without cellular service across Europe and Asia. According to estimates at the time, Ericsson may have faced SLA penalties equal to 100 million Euros.

The hidden cost of manual PKI management

Not all the negatives of manual PKI management are so obvious. Consider the labor costs of supporting a manual PKI process, for example.

Manually discovering, installing, monitoring, and renewing all digital certificates in an organization requires a tremendous amount of labor. The labor cost of installing just one manual SSL certificate is a multi-step process that can easily add up to more than $50 per web server. For an enterprise, this cost is multiplied by far greater numbers of servers, devices, and applications, quickly reaching astounding levels. If one employee makes a single mistake during those repetitions, widespread outages or breaches could result.

> *Manually discovering, installing, monitoring, and renewing all digital certificates in an organization requires a tremendous amount of labor.*

Enterprises choosing still to manually manage PKI already have costs and exposure to risk that are too high. Given the exponential growth of remote workers, cloud infrastructures, and mobile devices, the risk for organizations that continue to rely on manual PKI management will only increase in the immediate future.

Certificate lifecycle management cuts risk and cost

Fortunately, every organization can choose to automate the management of its certificates using advanced CLM technology. Modern CLM solutions can simplify and accelerate this transition for almost any organization and address obstacles standing in the way.

Enterprises that move to automated CLM solutions:

- Can allocate and manage certificates of all types on demand.

- Reduce certificate management costs.

- Can automatically detect and replace certificates coming up for expiration, eliminating costly outages.

- Swiftly and consistently authenticate new devices added to the infrastructure, eliminating the human error and increasing scalability.

- Significantly bolster overall security will be against malicious actors and malware, both known and unknown.

For these reasons, automated CLM of private and public PKI-based certificate authentication is a game-changing opportunity for most enterprises. The result? A far more secure, affordable, and easily managed identity security solution.

Preventing document fraud in a world built on digital trust

Martin Rehak

CEO, Resistant AI

All digital markets are built on trust and that trust has been reduced to an algorithm driven by proof of identity, which currently remains heavily reliant on formal documents such as a passport or driving license. Anyone looking to misrepresent who they are, where they live or what they're paid would need their documentation to reflect this false version of their status.

Highly automated workflows used by financial services are particularly vulnerable to this type of manipulation. Bank statements that are used to support lending applications, "know your customer" (KYC) procedures and other identity-driven financial purposes worldwide are regularly tampered with. In addition, "know your user" (KYU) processes, which include merchants, fintech companies and the B2B ecosystem, among others, are also subject to fraud.

> *Bank statements that are used to support lending applications, "know your customer" (KYC) procedures and other identity-driven financial purposes worldwide are regularly tampered with.*

A range of challenges

The challenges facing fraud prevention teams are significant. In the physical world, trust develops over time and generally begins with an introduction - a process that can be accelerated when accompanied by a recommendation or via a source who is already trusted. From that point onwards, the value of the relationship is determined by the way that people subsequently behave towards each other.

In the digital context, however, trust can't be based on a feeling - it must be represented by the data contained in documents and the rules attached to that data. What's more, the sheer number of transactions (i.e., behaviors whereby the value of the relationship is determined) being processed across today's complex financial networks, means this digital trust must be assessed at an appropriate pace. To meet these needs, automation has replaced manual human involvement, and while these technologies have brought many benefits to the process, they also present opportunities for people looking to commit fraud.

What are organizations, their fraud prevention teams and automation technologies up against?

Among the various methods used by those committing criminal fraud, an alarmingly common and effective tactic designed to defeat many existing automated technologies is the use of "synthetic identities." This is where real and fictitious identity fragments are combined specifically to evade fraud detection processes.

> *Among the various methods used by those committing criminal fraud, an alarmingly common and effective tactic designed to defeat many existing automated technologies is the use of "synthetic identities."*

The approach is increasingly sophisticated, with criminals employing complex, long-term strategies to build a credible credit history over time - sometimes over a period of years. With this in place, their aim is to carry out perhaps one major fraud before abandoning the identity entirely. As a result, this kind of activity is contributing to online payment fraud losses which are expected to exceed $206 billion cumulatively from the period between 2021 and 2025.

Next-generation automation

In working to prevent fraud, however, organizations have an important balance to strike: they have to reduce losses by protecting automated workflows, while simultaneously not making the experience inconvenient for customers.

> *Recent advances in artificial intelligence (AI), especially machine learning (ML), are giving fraud prevention teams the opportunity to meet the challenge head on.*

Recent advances in artificial intelligence (AI), especially machine learning (ML), are giving fraud prevention teams the opportunity to meet the challenge head on. For example, digital signature verification can be implemented using open-source software for machine learning.

However, detecting fraud within documents that have been digitally altered with graphics editors or "print-manipulate-scan" evasion techniques requires more sophistication.

Often undetectable to human fraud specialists, building an automated solution requires specialist knowledge of the metadata and digital footprints left by scanning and printing devices.

While these more advanced ML techniques work with most document types, they will typically deliver somewhere between 75% and 80% accuracy. This is a step in the right direction, but still not at a level where automation is reaching its potential. Instead, more specialized modelling is generally required.

Even more sophisticated and bespoke visual and structural modelling can be used to assess the look and feel of specific types of documents provided by third parties. This process compares them against examples of authentic documents provided by document originators, such as those from banks, utility companies, and government agencies.

Context-aware machine learning

The most recent and powerful generation of risk management and monitoring systems also employ context-aware machine learning. Instead of making decisions in isolation, each new customer interaction or transaction is assessed by considering all previous interactions between all other counterparties. The more data the system has to work with, the more accurate the assessments become.

The same contextual approach can be applied to document intake. Looking beyond single documents for signs of manipulation across multiple documents at once can reveal patterns indicative of serial or organized fraud.

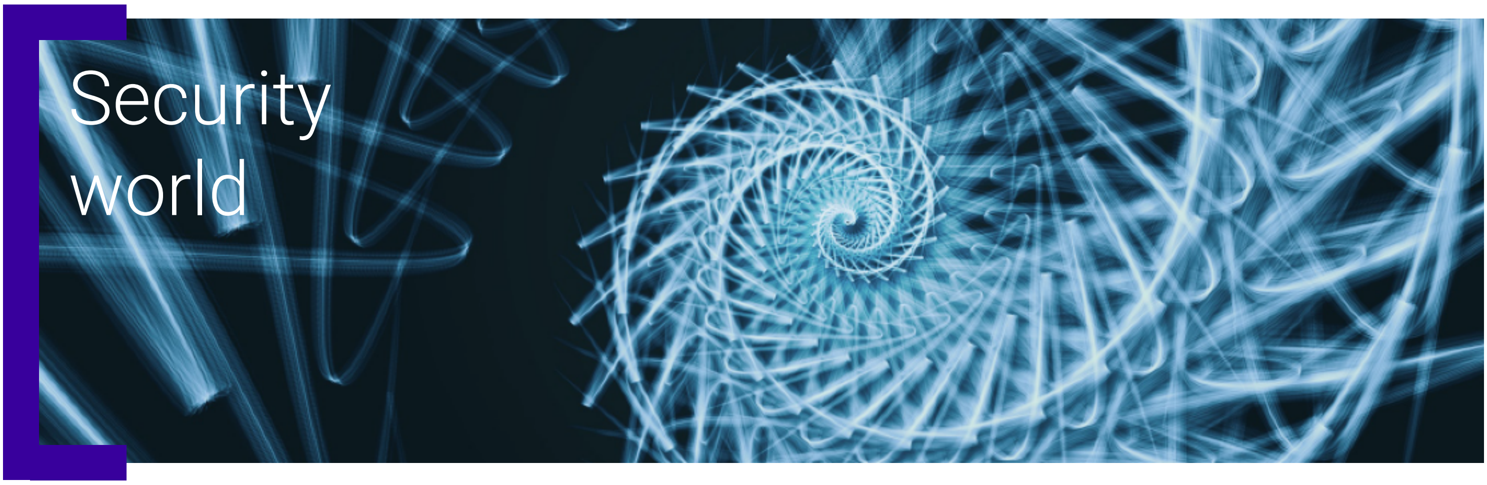
By concurrently using different models across a variety of use cases, including fraud (identities, account takeover, hoarding, basket switching) and money laundering (layering and integration), contextual analysis scores customers across a risk spectrum whose tolerance can be set to reflect an organization's appetite for risk.

For example, when an account is first opened, KYC checks establish customer identity, and that customer is assessed as "medium" risk by default. From that moment on, their behavior is continuously monitored and their risk rating adjusted accordingly based on the models' understanding of the characteristics and impact of different types of risk.

> *If automation is going to play a full role in allowing organizations to balance fraud prevention against the customer experience, they will need to draw on next-generation, AI and ML powered solutions.*

Fraudulent activities continue to evolve as criminals seek to evade detection to exploit the limitations of many current systems and processes, undermining the trust on which digital markets are built.

If automation is going to play a full role in allowing organizations to balance fraud prevention against the customer experience, they will need to draw on next-generation, AI and ML powered solutions. Those that do so will be ideally placed to minimize the costs they are forced to incur daily due to fraud.

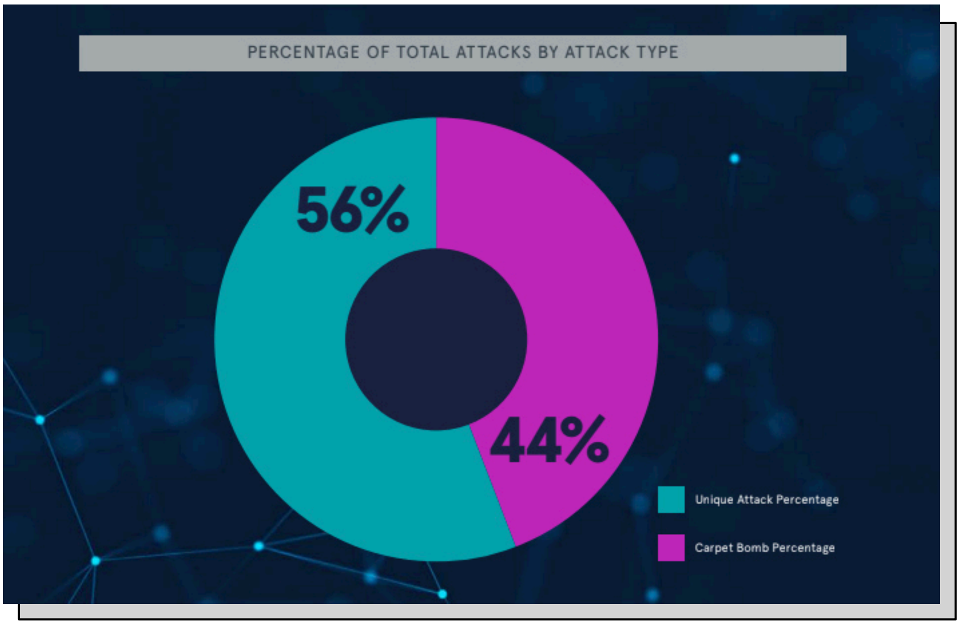


Carpet bombing DDoS attacks spiralled in 2021

Neustar Security Services has released a report which details the ongoing rise in cyberattacks in 2021, with an unprecedented number of carpet bombing distributed denial of service (DDoS) attacks.

Carpet bombing, in which a DDoS attack targets multiple IP addresses of an organization within a very short time, accounted for 44% of total attacks last year, but the disparity between the first and second half of 2021 was stark. While carpet bombing represented 34% of total attacks mitigated in both Q1 and Q2, these attacks saw a big jump in the second half – representing 60% of all attacks in Q3, and 56% in Q4.

While the vast majority of attacks fell into the 25 gigabits per second (Gbps) and under size category, and the average attack was just 4.9 Gbps last year, 2021 saw many large-scale attacks as well. The largest measured 1.3 terabits per second (Tbps) and the most intense was 369 million packets per second (Mpps).



The longest-lasting attack clocked in at 9 days, 22 hours and 42 minutes although the majority of attacks were over in minutes. Nearly 40% of the unique attacks seen by the SOC in 2021 took place in the first three months of the year. The number dropped significantly in the second and third quarters before rebounding in the fourth quarter.

How Log4Shell remediation interfered with organizations' cybersecurity readiness

(ISC)² published the results of an online poll examining the Log4j vulnerability and the human impact of the efforts to remediate it. Cybersecurity professionals from around the globe shared their experiences and opinions, revealing the severity and long-term consequences of the Log4j attack for both security teams and the organizations they protect.

There haven't been any major breaches attributed to Log4j to date, in large part due to the hard work and dedication of the cybersecurity community. According to the poll, as a result of the reallocation of resources and the sudden shift in focus that was required, security teams reported that many organizations were less secure during remediation and fell behind on their 2022 security priorities.

This landscape of unsteadiness is what the cybersecurity workforce gap looks like in practice. The gap stands at 2.72 million professionals globally, with 60% of respondents reporting that the workforce shortage is placing their organizations at risk.

When a cybersecurity team is staffed appropriately, the disclosure of severe vulnerabilities doesn't become a "fire drill" as the team has the resources to investigate and remediate in a timely manner. Investing in the development of existing staff is one of the many factors that contribute to higher retention.

What is challenging malware analysis?

OPSWAT announced a report which reveals that nearly every organization struggles with malware analysis. Specifically, 94% of organizations are challenged to find, train, and retain malware analysis staff.

Furthermore, 93% of organizations are challenged by malware analysis tools that lack automation, integration, and accuracy. Consequently, over 20% of organizations reported they were unable to investigate and resolve a majority of their malicious files or alerts. The report also found that 99% of organizations would benefit from additional capabilities for malware analysis.

Evidence from the report suggests that malware analysis is maturing as a business capability since nearly half of the organizations have a dedicated malware analysis function and more than half report intermediate capabilities, which would include sandbox tools for threat detection. However, nearly every organization struggles with the human element of malware analysis and the technical limitations of their existing solutions.

Solving the problem of secrets sprawling in corporate codebases

GitGuardian announced the results of its report which extends its previous edition focused on public GitHub by depicting a realistic view of the state of secretssprawl in corporate codebases.

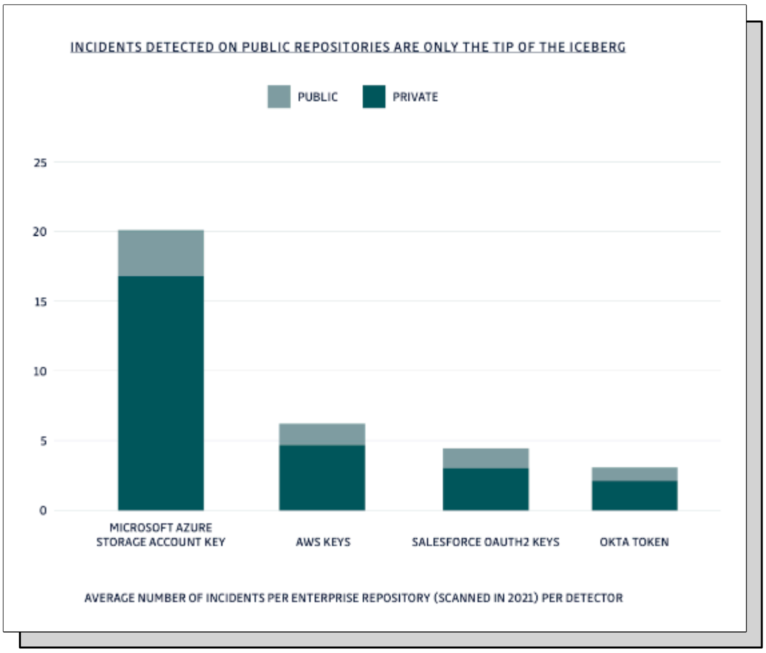
The data reveals that on average, in 2021, a typical company with 400 developers would discover 1,050 unique secrets leaked upon scanning its repositories and commits. With each secret actually detected in 13 different places, the amount of work required for remediation far exceeds current AppSec teams' capabilities (1 AppSec engineer for 100 developers).

When compared to open-source corporate repositories, private ones are also four times more likely to expose a secret, comforting the idea that they permeate a false sense of secrecy threatening security postures.

The historical volume of secrets-in-code, coupled with their constant growth, jeopardizes the remediation capacity of security teams, primarily application security engineers. This, in turn, puts the whole transition process to DevSecOps at risk. Therefore, an action plan is necessary to resolve this situation as soon as possible.

The report also highlights that the secrets sprawl phenomenon is mostly still in its infancy. First, improving on its prior results, public GitHub monitoring reported doubling the number of secrets leaked, reaching just over 6M in 2021. On average, 3 commits out of 1,000 exposed at least one secret, +50% compared to 2020.

By integrating vulnerability scanning into the development workflow, security isn't a bottleneck anymore. You can help developers catch vulnerabilities at the earliest stage and considerably limit remediation costs. This is even more true for secrets detection, which is very sensitive to sprawling (as soon as a secret enters a version control system, it should be considered compromised and requires remediation effort). You can thus reduce the number of secrets entering your VCS by better-educating developers while preserving their workflow.



70% of breached passwords are still in use

SpyCloud announced a report that examines trends related to exposed data. Researchers identified 1.7 billion exposed credentials, a 15% increase from 2020, and 13.8 billion recaptured Personally Identifiable Information (PII) records obtained from breaches in 2021.

Through its analysis of this data, it was found that despite increasingly sophisticated and targeted cyberattacks, consumers continue to engage in poor cyber practices regarding passwords, including the use of similar passwords for multiple accounts, weak or common passwords and passwords containing easy-to-guess words or phrases connected to pop culture.

The average consumer owns hundreds of online accounts, each with a unique login, and the unfortunate result is an increase in consumer password reuse. SpyCloud's report found that 64% of users with multiple compromised passwords reused similar passwords for multiple accounts, making them ripe for account takeovers and password spraying attacks. This represents a 4-point jump from the 2021 report.

The year over year increase in password reuse reflects the ease with which attackers can use one stolen password to compromise multiple accounts. More than 82% of the reused passwords analyzed consisted of an exact match to a previous password, and 70% of users tied to breaches last year and in years prior are still using an exposed password. Since 2016, SpyCloud has recaptured more than 25 billion total exposed accounts with passwords.

Organizations taking nearly two months to remediate critical risk vulnerabilities

Edgescan announces the findings of a report which offers a comprehensive view of the state of vulnerability management globally. This year's report takes a more granular look at the trends by industry, and provides details on which of the known, patchable vulnerabilities are currently being exploited by threat actors.

The report reveals that organizations are still taking nearly two months to remediate critical risk vulnerabilities, with the average mean time to remediate (MTTR) across the full stack set at 60 days.

High rates of "known" (i.e. patchable) vulnerabilities which have working exploits in the wild, used by known nation state and cybercriminal groups are not uncommon.

Remote access exposures across the attack surface are a worrying trend and accounted for 5% of total attack surface exposures in 2021.

Crucially, 57% of all observed vulnerabilities are more than two years old, with as many as 17% being more than five years old. These are all vulnerabilities that have working exploits in the wild, used by known nation state and cybercriminal groups. Edgescan also observed a concerning 1.5% of known, unpatched vulnerabilities that are over 20 years old, dating back to 1999.

Cybercrime getting more destructive, remote workers in the crosshairs

Fortinet's threat intelligence from the second half of 2021 reveals an increase in the automation and speed of attacks demonstrating more advanced persistent cybercrime strategies that are more destructive and unpredictable.

In addition, the expanding attack surface of hybrid workers and hybrid IT is a focal point that cyber adversaries are attempting to exploit.

The Log4j vulnerabilities that occurred in late 2021 demonstrate the rapidly increasing speed of exploit that cybercriminals are attempting to leverage to their advantage. Despite emerging in the second week of December, exploitation activity escalated quickly enough, in less than a month, to make it the most prevalent IPS detection of the entire second half of 2021.

The prevalence of ELF and other Linux malware detections doubled during 2021. This growth in variants and volume suggests that Linux malware is increasingly part of adversaries' arsenal. Linux needs to be secured, monitored and managed as any other endpoint in the network with advanced and automated endpoint protection, detection and response. In addition, security hygiene should be prioritized to provide active threat protection for systems that may be affected by low-lying threats.

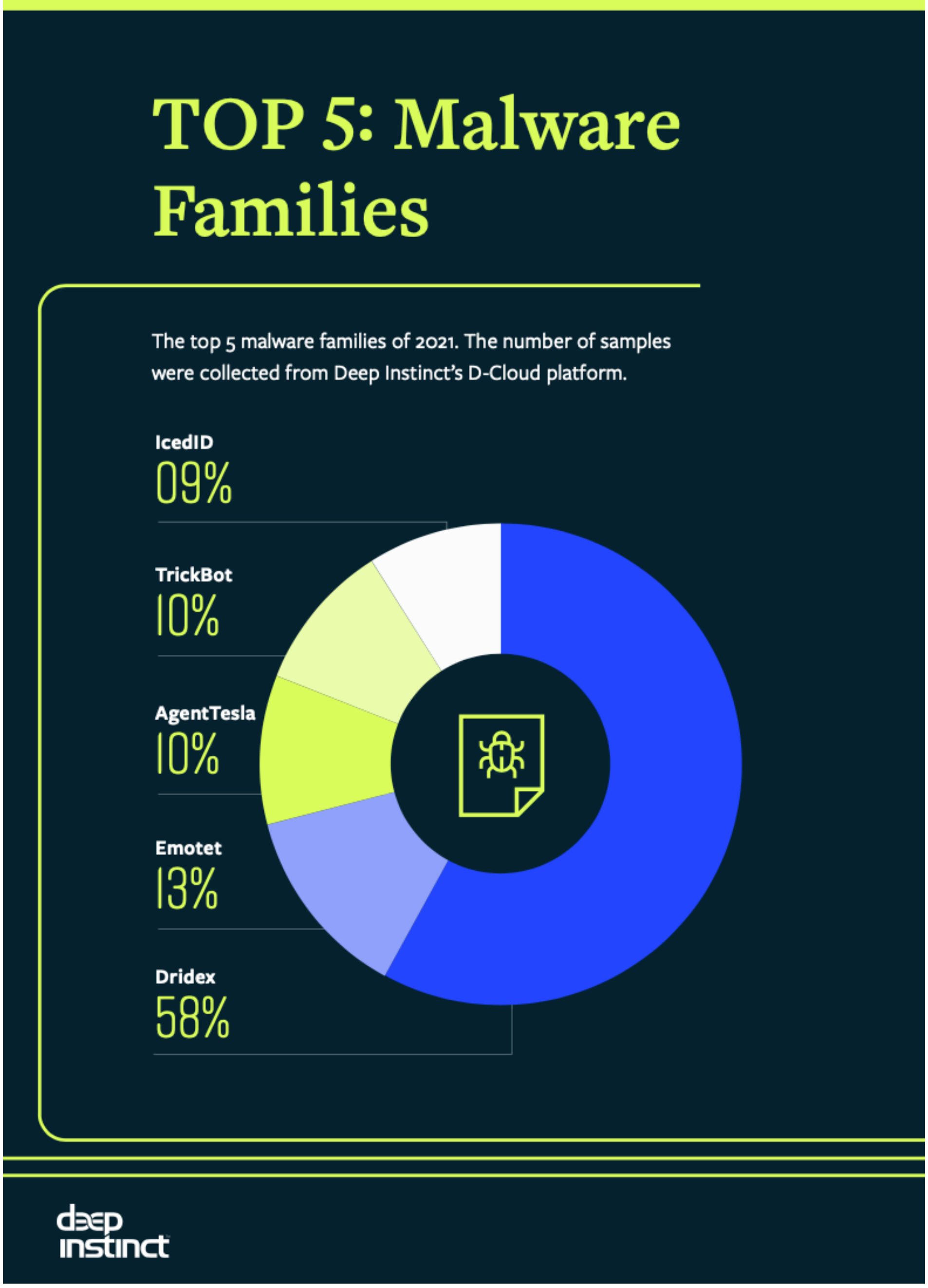
Evaluating the prevalence of malware variants by region reveals a sustained interest by cyber adversaries in maximizing the remote work and learning attack vector. In particular, various forms of browser-based malware were prevalent. This often takes the form of phishing lures or scripts that inject code or redirect users to malicious sites.

Data reveal that ransomware has not subsided from peak levels over the last year and instead, the sophistication, aggressiveness, and impact of ransomware is increasing. Threat actors continue to attack organizations with a variety of new as well as previously seen ransomware strains, often leaving a trail of destruction.

Bad actors are becoming more successful at evading AI/ML technologies

Deep Instinct Threat Research team extensively monitored attack volumes and types and then extrapolated their findings to predict where the future of cybersecurity is heading, determine what motivates attackers, and most importantly, lays out the steps organizations can take now in order to protect themselves in the future.

One of the most pronounced takeaways from this research on 2021 threat trends is that bad actors are becoming more successful at evading AI/ML technologies, prompting organizations to redouble efforts in the innovation race.



TOP 5: Malware Families

The top 5 malware families of 2021. The number of samples were collected from Deep Instinct's D-Cloud platform.

Specific attack vectors have grown substantially, including a 170% rise in the use of Office droppers along with a 125% uptick in all threat types combined. The volume of all malware types is substantially higher versus pre-pandemic.

In addition, threat actors have made a discernable shift away from older programming languages, such as C and C++, in favor of newer languages, such as Python and Go. Not only are these newer languages easier to learn and to program versus their predecessors, but they also have been less commonly used and are therefore less likely to be detected by cybersecurity tools or analyzed by security researchers.

IoT security is foundational, not optional

A PSA Certified report predicts that this year will mark a turning point in securing the Internet of Things (IoT), as the industry collectively commits to addressing the historic lag between the rate of digital transformation and the speed of securing the ecosystem.

The annual barometer of industry perceptions and intentions around IoT security surveyed 1,038 technology decision makers across Europe, USA, and APAC, and signals a positive turning point for security with organizations placing it at the center of IoT strategy and organizational culture.

90% of respondents have increased the importance placed on security in the past 12 months, almost 9 in 10 deem security in their top three business priorities and 42% of those rank building a 'security-first culture' as their top organizational priority.

The study indicates that increased consumer expectations and growing cyber risk are largely driving the change. Debunking the myth that consumers are purely driven by product features and price, 83% of respondents state they look for specific security credentials when buying connected products. Over a third of companies believe distributed working has increased the likelihood of an IoT hack and one in five respondents work for companies that had been victims of hacks due to vulnerabilities in third-party products or services.

Not only is a security-first culture deemed critical to protecting businesses against cyber-risk, it's also recognized as a driver of commercial value. 96% of tech decision makers say that having security in their products positively impacts the bottom line, with nearly seven in ten citing they can charge a premium for built-in security.

Cybercriminals seeking more than just ransomware payment

Venafi announced the findings of a global survey of IT decision-makers looking into the use of double and triple extortion as part of ransomware attacks. The data reveals that 83% of successful ransomware attacks now include alternative extortion methods, such as using the stolen data to extort customers (38%), exposing data on the dark web (35%), and informing customers that their data has been stolen (32%).

Just 17% of successful attacks solely asked for a ransom in return for a decryption key, meaning that many new forms of extortion are now more common than traditional methods. As data is now being exfiltrated, having a back-up of data – while still essential for recovery from an attack – is no longer effective for containing a breach.

When asked about the evolution of extortion in ransomware attacks, 71% of those polled believe that double and triple extortion has grown in popularity over the last 12 months, and 65% agree that these new threats make it much harder to say no to ransom demands.

This is creating problems for the industry. 72% of IT decision-makers agree that ransomware attacks are evolving faster than the security controls needed to protect against them, and 74% agree that ransomware should now be considered a matter of national security. As a result, 76% of companies are planning on spending more in 2022 on ransomware-specific controls due to the threat of double and triple extortion.

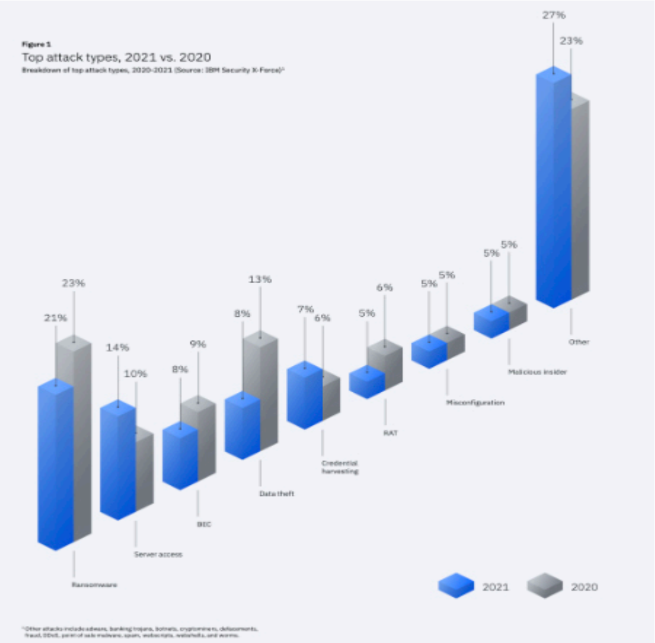
Ransomware wreaked havoc last year, manufacturing was most targeted

IBM Security released its annual X-Force Threat Intelligence Index unveiling how ransomware and vulnerability exploitations together were able to “imprison” businesses in 2021 further burdening global supply chains, with manufacturing emerging as the most targeted industry.

While phishing was the most common cause of cyberattacks in general in the past year, there was a 33% increase in attacks caused by vulnerability exploitation of unpatched software, a point of entry that ransomware actors relied on more than any other to carry out their attacks in 2021, representing the cause of 44% of ransomware attacks.

The 2022 report details how in 2021 ransomware actors attempted to “fracture” the backbone of global supply chains with attacks on manufacturing, which became 2021’s most attacked industry (23%), dethroning financial services and insurance after a long reign. Experiencing more ransomware attacks than any other industry, attackers wagered on the ripple effect that disruption on manufacturing organizations would cause their downstream supply chains to pressure them into paying the ransom.

An alarming 47% of attacks on manufacturing were caused due to vulnerabilities that victim organizations had not yet or could not patch, highlighting the need for organizations to prioritize vulnerability management.



Small business owners worried about the cybersecurity of their commercial vehicles

Small business owners are adding electric vehicles to their service fleets, a survey released by HSB reports, but they worry about cybersecurity when connecting them to public charging stations.

76 percent of those business owners and managers were concerned EV charging stations could be a target for hackers, ransomware, and other cyber-attacks.

The plug-in electric chargers communicate with vehicles through an internet connection and security experts warn the systems could be hacked.

These potential threats add to the concerns of small business owners, who were already worried about the cybersecurity of their commercial vehicles.

The survey found 46 percent were somewhat or very concerned about the cyber exposures and safety of internet connected and automated vehicles.

56 percent of them are somewhat or very concerned their vehicles could be immobilized or made inoperable, their safety compromised (54 percent), and that a hacker could communicate and confront them over their audio system (43 percent).

The importance of building in security during software development

Checkmarx released the UK findings of its report which found that 45% of organizations have suffered at least two security breaches as a direct result of a vulnerable application. Alongside this, the report discovered 34% of UK organizations who had experienced a security breach relating to an application in the year preceding the survey have laid off employees seen as bearing responsibility.

Respondents of the survey also noted those who often bear the most responsibility for the security of applications as software developers (39%), and application security managers (32%). Only 10% stated CISOs or CSOs as those with the most responsibility within their organization.

Given 45% of respondents – which consisted of AppSec managers and software developers in UK organizations of over 1,000 employees – reported being breached twice in the last 12 months. With 22% having been breached three times, the survey has made it clear that security teams may be at risk, with organizations not adverse to penalising those deemed responsible for such security breaches.

The survey also looked at what led to these breaches, with 43% of respondents stating they suffered a software supply chain attack, an attack vector known to be a firm favourite among malicious threat actors.

API security: Understanding the next top attack vector

Matt Tesauro

Director of Security Evangelism,
Noname Security

Application Programming Interfaces (APIs) underpin today's digital ecosystem as the essential connective tissue that allows companies to exchange data and information quickly and securely. As the post-pandemic world leans heavily on digital interaction to maintain user connections, the volume of API traffic has grown rapidly. However, this growth has also brought on emerging security challenges.

While traditional application security controls remain necessary, they are not quite up to the API security challenge. Fortunately, there are certain basic API security practices organizations can implement to create a more resilient API security posture.

What is threatening API security?

When contemplating API security, you must consider its risks and exposures. Hackers spend more time poking at APIs than most companies do maintaining them. It is rare to see an attacker "break" an API. Rather, the most common threat vector is misconfigurations and weak links between APIs deployed in each piece of software.

> *Hackers spend more time poking at APIs than most companies do maintaining them.*

The first step in fixing the API security problem isn't necessarily a new testing solution, but rather taking stock of how many APIs an organization has deployed and how they are interacting with one another. Each API is unique and needs individual attention and detailed understanding. Without visibility into the nature and scope of its API deployments, an organization will find itself hamstrung at the earliest stage in attempting to tackle its API security risk.

Another challenge facing security practitioners when implementing API security programs are unclear roles and responsibilities for security teams. This commonly cited issue means that there are gaps in API maintenance, monitoring and security, and they become doorways for hackers to come in. Teams need to be given specific responsibilities regarding API security maintenance to ensure that nuanced differences between APIs are addressed.

What can companies do to ensure they are prioritizing API security?

The original security problems stemmed from a misunderstanding of an API's software-to-software communication. With organizations often having hundreds or even thousands of APIs in use, the task of securing them all is highly complex. The challenge requires a strategic approach for security assessment that can be applied universally and efficiently across a diverse set of APIs.

One example of this type of strategy is D.A.R.T., which stands for Discover, Analyze, Remediate, and Test.

D.A.R.T. serves as both a lens to view security challenges, as well as a litmus test to measure the effectiveness of security efforts and solutions. This solution addresses security across the API ecosystem, from code to production, and needs to be used for each API's unique individual requirements.

- **Discover:** This encompasses the ability to find and inventory all APIs. Enterprises manage thousands of APIs, and many of them are not routed through a proxy or API gateway. APIs that are not routed are not monitored, are rarely audited, and are most vulnerable to mistakes which lead to attacks. It is important to create a complete API inventory enabling the team to discover and assess every API, including legacy and shadow APIs with data classification.

- **Analyze:** The ability to detect API anomalies, changes and misconfigurations is vital. It's important for enterprises to analyze API access, usage, and behavior. Leveraging AI and ML for automated behavior analysis helps to identify issues in real-time. When considering existing detection capabilities or those of an API security vendor, companies must remember they will only be as effective as their ability to discover a complete inventory of APIs.

- **Remediate:** The next step is to have the ability to resolve detected anomalies and misconfigurations. Based on that inventory, teams can begin remediation by identifying misconfigurations and vulnerabilities in the source code, network configuration and policy. Teams can focus on security interventions in the highest-risk areas and provide an effective detection and response. The implementation of automated and semi-automated blocking and remediation of threats means that they can be blocked from even happening.

- **Test:** Even if a detection and response system is implemented, it is important to have continuous testing of the different API endpoints to identify API risks before they emerge. Analyzing APIs and remediating issues while in development allows companies to deploy APIs with complete confidence and trust.

The road ahead

2022 will be the year of the API security "arms race," as security teams and hackers alike bring more sophisticated technologies to the playing field.

Hackers are increasingly turning their attention towards APIs as an attack vector and will undoubtedly develop more advanced tools and methods for exploitation. Hackers have shown that they have and will continue to batter down the doors of companies through their insecure APIs.

Security teams that are too reliant on tools, have unclear roles and responsibilities and do not execute routine API maintenance may be doing their organizations more harm than good.

Taking the time to get educated on specific strategies such as D.A.R.T, ensures that each API is properly managed and secured.

Runecast

How CISOs & CIOs enable IT Security & Ops teams with **proactive** issues discovery

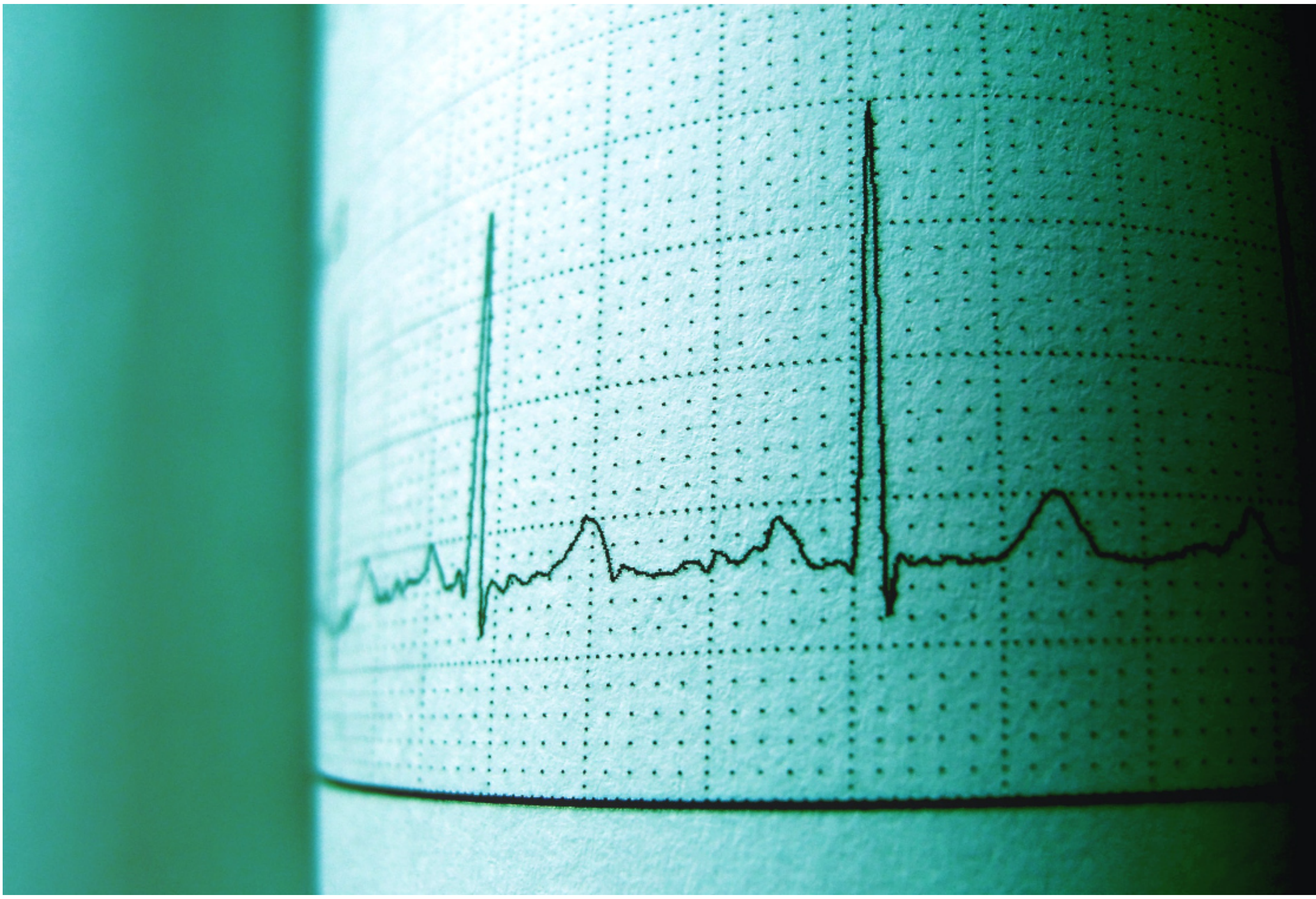
Take the Runecast Challenge
(for VMware)

Previously unknown issues uncovered or 12 months on us*

TAKE THE CHALLENGE NOW

www.runecast.com

* See full Terms & Conditions on the website.



The evolution of security analytics

Saryu Nayyar

CEO, Gurucul

As networks continue to evolve and security threats get more complex, security analytics plays an increasingly critical role in securing the enterprise. By combining software, algorithms and analytic processes, security analytics helps IT and security teams proactively (and reactively) detect threats before they result in data loss or other harmful outcomes.

Given that the average time to identify and contain a data breach in 2021 was 287 days, it's more important than ever for organizations to include security analytics in their threat detection and response programs. But how has this technology changed over the last decade? In this article, I will explore the evolution and importance of security analytics.

> *By combining software, algorithms and analytic processes, security analytics helps IT and security teams proactively (and reactively) detect threats before they result in data loss or other harmful outcomes.*

This evolution has had two main trends.

First, security analytics is becoming more sophisticated. In the last 10 years the industry has transitioned from rule-based alerting to big data and machine learning analysis. Second, products have become more open and customizable.

As these technologies have advanced, so too have their specific use cases, with organizations using these for identity analytics (examining authentication, authorization and access for anomalies), fraud (finding anomalous transactions), and more. Today, security analytics plays a central role in Security Information and Event Management (SIEM) solutions and Network Detection and Response products (not to mention standalone security analytics software).

To better understand this evolution and the capabilities of current security analytics solutions, let's dive into the three primary generations of security analytics advancement.

Generation one

Traditional security analytics focused on correlation and rules within a proprietary platform.

Users imported data into a closed database, the data was normalized and run through a correlation engine, and then the system produced alerts based on rules. Products typically included alert enrichment, which provided more useful context along with an alert, such as linking it to a specific user, host, or IP address.

However, this era often suffered from "alert fatigue" where the analytic solution produced more alerts than the security team could investigate, including high numbers of false positives. Sorting which alerts were important and which ones weren't involved a great deal of manual work. Furthermore, these solutions were often entirely proprietary, with little to no options for customization. This prevented the security team from tweaking rules to cut down on the number of bad alerts. They were stuck with the alert fatigue issue.

Generation two

The second generation of security analytics began to incorporate big data and statistical analysis, while remaining a black box to users.

These solutions offered data lakes instead of databases, which allowed for a greater variety of data to be gathered and analyzed, but they were still proprietary. New analytics capabilities emerged, such as the ability to include cloud data, network packets and flow data, but users still couldn't see how they worked or verify the results.

Data enrichment was better, but users largely could not customize the contextual data they wanted with their alerts. For example, a security team might want to add asset criticality data so they can prioritize events that affect key pieces of their infrastructure or include information from external sources like VirusTotal.

Many solutions started offering threat hunting capabilities as well, which made it easier for security teams to proactively search for suspicious activity that evaded perimeter security controls.

But false positives and limited bandwidth on security teams continued to be a major challenge. In fact, this remains a challenge today. According to the 2021 Insider Threat Report from Cybersecurity Insiders, 33% of respondents said the biggest hurdle to maximizing the value of their SIEM was not having enough resources and 20% said too many false positives.

Generation three

The third generation of security analytics technologies brings us to the current day, where machine learning, behavioral analysis and customization are driving innovation.

There are now SIEM products that allow organizations to use their existing data lakes, rather than forcing customers to use proprietary ones. And some solutions have opened their analytics, enrichment, and machine learning models so users can better understand them and modify as needed.

> *Security analytics have evolved quickly in recent years and as we look ahead, the industry is starting to combine SIEM, User Entity Behavioral Analytics (UEBA), Security Orchestration, Automation and Response (SOAR) and Extended Detection and Response (XDR) for a more automated and telemetry rich approach to threat detection and response.*

Today, powerful algorithms find patterns in data, set baselines and identify outliers. There's also a greater focus on identifying anomalous behavior (a user taking suspicious actions) and on prioritizing and ranking the risk of alerts based on contextual information like data from Sharepoint or IAM systems. For example, a user accessing source code with legitimate credentials might be a low-priority alert at best, but that user doing so in the middle of the night for the first time in weeks from a suspicious location should trigger a high-priority alert. Thanks to these capabilities, analytic solutions are reaching the point where they can trigger remediation actions automatically.

Security analytics have evolved quickly in recent years and as we look ahead, the industry is starting to combine SIEM, User Entity Behavioral Analytics (UEBA), Security Orchestration, Automation and Response (SOAR) and Extended Detection and Response (XDR) for a more automated and telemetry rich approach to threat detection and response.

> *Open access to security analytics is also a monumental shift that helps teams better understand and tweak these solutions so they can verify models and generate better results.*

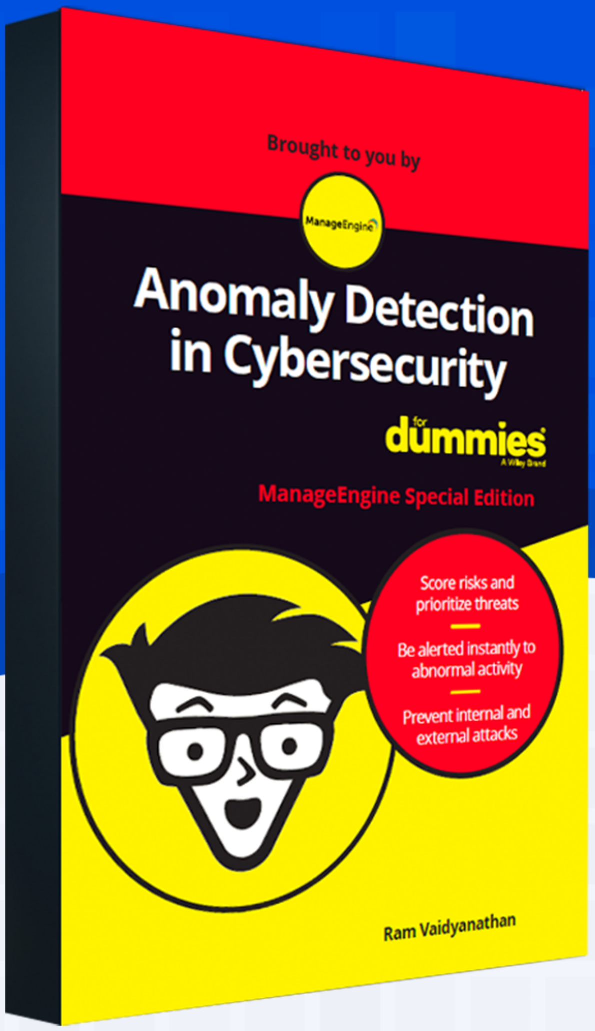
But today, the latest advancements are helping to reduce the workload on security teams, allowing them to better detect and contain both known and unknown threats more quickly. Open access to security analytics is also a monumental shift that helps teams better understand and tweak these solutions so they can verify models and generate better results.

Ideally, analytics solutions should have strong pre-built libraries of machine learning models that don't require users to be data scientists to edit them (but give them the editing option if needed).

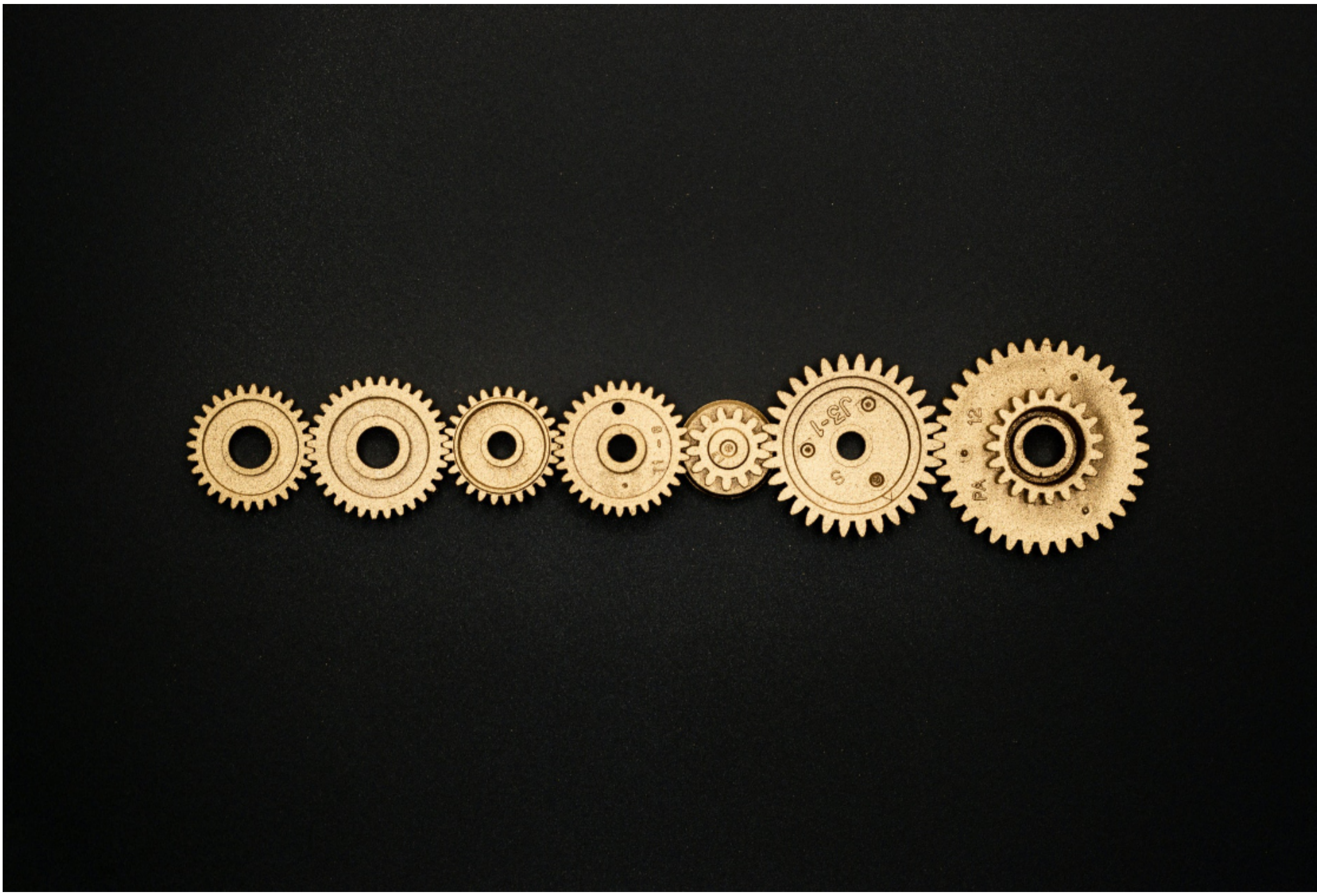
As these capabilities continue to develop, I believe they'll be a key factor in helping security teams reduce that 287-day average time to contain a breach in the coming years.

ManageEngine
Log360

Anomaly Detection in Cybersecurity for Dummies


Brought to you by
ManageEngine
Anomaly Detection in Cybersecurity
for dummies
A Wiley Brand
ManageEngine Special Edition
Score risks and prioritize threats
Be alerted instantly to abnormal activity
Prevent internal and external attacks
Ram Vaidyanathan

GRAB YOUR FREE COPY NOW!



Supply chain cybersecurity: Pain or pleasure?

Sean Arrowsmith

Director, Crossword Cybersecurity

Whatever sector your business operates in, you will depend on third parties to provide you with goods and services to support what you do. Whether you are a small printing services company working with an accountant or an organization with a full manufacturing and distribution supply chain, suppliers are important to your daily operations and will all on some level interact on site or digitally with your business, and this makes them a risk vector.

Companies deal with these risk vectors by restricting the access these individuals have, such as stopping them gaining access to certain areas, or using network and IT resources. Yet, while it is common for IT departments to assess the official suppliers that a company might use for areas such as cloud services, it remains a longstanding business challenge to monitor the cybersecurity risks from suppliers across a company's whole supply chain.

> *Cyber attacks have become so advanced that the starting point of an attack is often not the primary target, but the weakest part of the underlying supply chain.*

At a fundamental level, to mitigate cybersecurity risk, a company must be assured that every supplier they work with is on top of protecting the security of the data, and the availability of the services with which they are entrusted. Cyber attacks have become so advanced that the starting point of an attack is often not the primary target, but the weakest part of the underlying supply chain.

Assessing the risks

Many organizations use manual processes for their cybersecurity based supplier assessments, sending spreadsheet, Word, or PDF questionnaires by email, but this quickly becomes a cumbersome manual process, and itself can be regarded as a cybersecurity risk. Mistakes happen, processes become drawn out, and it is very easy for suppliers to not be checked at the frequency they should or be forgotten altogether.

Of even greater risk is that manual processes make it harder for organizations to gain an overall picture of where cyber risks sit in the supply chain. If data is not collated and assessed regularly, then a supplier failing to meet a requirement may go unchecked. Worse still, systemic risks across the supply chain may leave the organization exposed to a catastrophic cyber event. When such an event occurs, it is already too late.

Whether cybersecurity, financial or other regulatory controls, organizations need a more reliable approach to reduce risks associated with suppliers, vendors and other third parties.

A standardized, automated approach

A good framework for supplier assurance requires procurement teams, IT teams and other departments to work together to ensure they understand each other's domains, objectives and responsibilities in terms of cybersecurity and regulatory compliance. A starting point is for them to jointly develop Supplier Impact criteria that systematically assess how much inherent risk every supplier or third party may have in that department's sphere.

Each supplier can then be measured against these criteria, and their supplier impact level established. A different approach for each level of impact should be agreed jointly and completely standardized across the organization.

For example, for suppliers with a Very High impact, the supplier should be expected to demonstrate a high level of internal controls. With cybersecurity, for example, this means obtaining or working to achieve high standards such as ISO27001, IASME Governance or NIST. It is the supplier's responsibility to show a serious level of control rather than the hard-pressed cybersecurity team's responsibility to dive into hundreds of hours of audit work. These standards also have the benefit of being easy for a non-cyber specialist to determine if the standard is present or not.

Where a technical assessment or test is needed, such as a penetration test by a credible third party, then the supplier assurance team can be responsible for making sure that this takes place – handing over the responsibility to the cyber teams or external testers where needed. This "management of risk" role cannot be handed over though, as tempting as it is when the talk gets incomprehensibly technical.

The approach at each level of supplier impact should also include ongoing assessments. A lot of companies think “assure when you procure” is enough. But with the pace of modern business and the speed of change, there must be a regular assessment routine to stay on top of the risks. Again, the supplier assurance team can timetable and manage these ongoing reviews and focus on the governance of third-party risk – whether cyber, continuity, financial or regulatory – but executed by those with the domain expertise to speak with their counterparts in the supply chain.

> *A lot of companies think “assure when you procure” is enough. But with the pace of modern business and the speed of change, there must be a regular assessment routine to stay on top of the risks.*

Taking the pain out of supply chain cybersecurity

Taking a formulated and strategic approach to managing supply chain cybersecurity and wider compliance issues, creates an environment where the different teams involved in supplier risk start to use shared information systems to record and visualize supplier risks.

> *Introducing an online platform to automate supplier assurance makes the whole process efficient and more secure.*

Introducing an online platform to automate supplier assurance makes the whole process efficient and more secure. Users have a single source of information and can create impressive supplier scorecards showing a combined view of financial, cyber, GDPR, Slavery and other risks all on one simple chart for each supplier. This provides a shared understanding of the totality of risk from each supplier and helps specialist teams - such as IT and the supplier assurance team – to understand how their worlds fit together.

By formalizing supplier assurance processes and using technology to facilitate their execution across all domains, cyber assessments become part of the rhythm of the whole supplier management process. In this way, companies can have confidence in the strength of the supply chain, mitigate cyber risks and take a lot of the pain out the experience.

+ HELPNETSECURITY

INDUSTRY NEWS

Find the latest news about products, executive appointments, partnerships, and more.

helpnetsecurity.com

A 2022 priority: Automated mobile application security testing

Ryan Lloyd

Chief Product Officer, Guardsquare

The use of mobile devices has skyrocketed in the past two years and with it the mobile app market. It's predicted mobile apps will generate more than $935 billion in revenue by 2023.

Areas with growth potential, unfortunately, often attract the attention of threat actors looking to exploit vulnerabilities for financial gain. That's why mobile app security has become a critical area of focus across industries - especially if the organization has an app that contains valuable intellectual property (IP) or has sensitive data passing through it.

Implementing security measures throughout the app development process and continuing to monitor the app once it's released into the wild is what ultimately keeps your mobile app secure and your business safe.

Mobile application security testing will be a priority for any organization with a mobile app in 2022. To understand why, let's look at the typical security threats mobile apps encounter and the impact these threats can have on an organization.

Mobile application security threats

Mobile applications are susceptible to some unique threats.

Consider, for example, the MATE (man-at-the-end) attack vector. An attacker can load a mobile application on their local device and then use specialized tools and resources to inspect and reverse engineer the application. This gives them access to the "secret sauce" of how the app runs.

Though mobile app security threats can range in severity and sophistication, the outcome is often the same: data leakage, theft of IP, loss of revenue, and loss of customer trust.

Other mobile app security vulnerabilities include insecure data storage, security misconfigurations, and insecure communication, all of which align to the OWASP Top 10 mobile risks list. Without multiple layers of protection, your application can easily fall victim to a variety of threats.

Though mobile app security threats can range in severity and sophistication, the outcome is often the same: data leakage, theft of IP, loss of revenue, and loss of customer trust. That's why mobile app security needs to be a focus at every stage of the mobile app development lifecycle.

Enter mobile app security testing

When mobile app security includes frequent testing to obtain real feedback, mobile app developers are better prepared to identify and mitigate mobile app security threats and vulnerabilities.

Mobile app security testing is the process of scanning your app to identify potential security issues that could impact your mobile application. Though specific needs for app scanning may vary, whether driven by compliance or in response to a security incident, the goal is to effectively harden the application and mitigate risk.

When mobile app security includes frequent testing to obtain real feedback, mobile app developers are better prepared to identify and mitigate mobile app security threats and vulnerabilities.

There are two ways to think about testing an application: static analysis and dynamic analysis. Though both are uniquely effective, when combined, they can substantially increase the security posture of your mobile app.

Why penetration testing won't cut it

Traditionally, mobile teams have leaned on pentesting as a preferred form of mobile app testing. Though an effective security assessment approach — pentesting can identify the absence of code hardening and anti-tampering protection — it doesn't always work in the fast-paced world of mobile app development.

Pentesting is expensive and slow. The findings are usually shared with the development team outside the actual software development process, sometimes months later. This often requires the organization to make a tough decision: Is it more important to publish the app on time or address the risks identified?

If the risk is determined to be manageable, the feedback may not get implemented. But if the risk is high enough, development teams will need to drop everything to fix it, causing a ripple effect into the development and release of new app features. It's easy to see how this process can put security teams and mobile app development teams in opposition to each other.

This also emphasizes the importance of identifying and selecting a security testing tool that is designed specifically for mobile applications and built for developers. A developer-friendly mobile security tool offers actionable feedback that better aligns development and security teams.

Automated app security testing and why it will be a priority

In a world where organizations are tasked with constant innovation to meet their customers' rapidly changing demands, organizations can't risk the fallout of an unsecured app.

In 2022, we anticipate app security testing will likely become a responsibility of the mobile app development team, done through the support of automated tools. This makes the testing process cost-effective and manageable, so development teams get frequent and regular feedback on the security of a mobile app.

An added benefit? An automated testing tool enables developers to conduct mobile app testing as frequently as they want (or need) to, setting the team up for an efficient, successful external assessment or pen test.

> *In 2022, we anticipate app security testing will likely become a responsibility of the mobile app development team, done through the support of automated tools.*

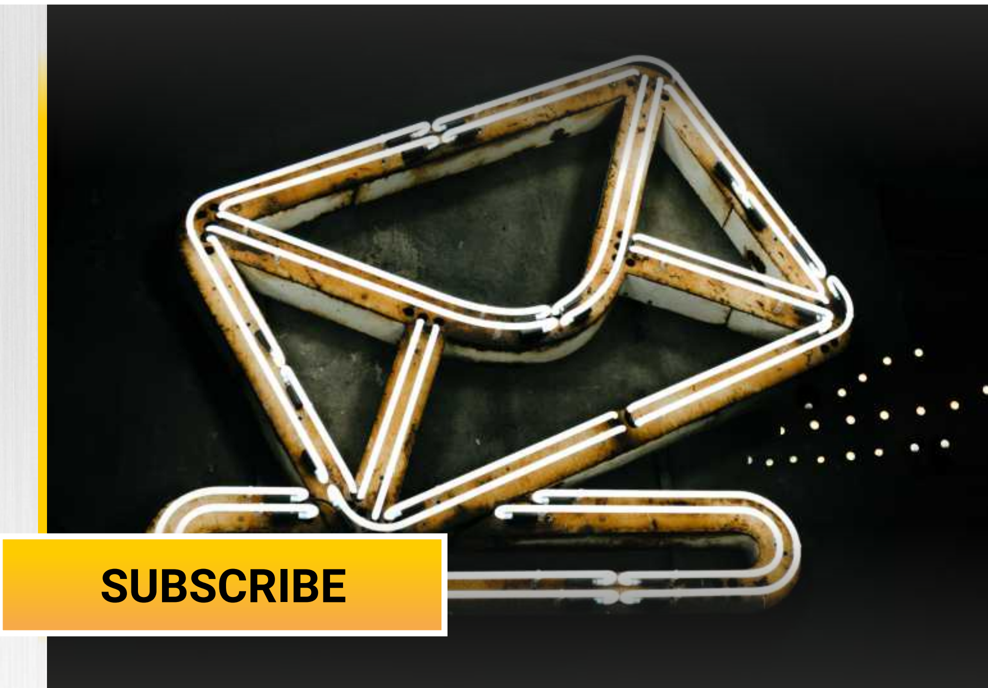
Mobile apps are increasingly becoming the main way users interact with businesses. Prioritizing application security scanning in 2022 will enable organizations to take proactive steps to prevent data leakage, IP theft, loss of revenue, and reputational damage.

HELP NET SECURITY WEEKLY NEWSLETTER

E-mail sent every Monday with a recap of the last 7 days

HELPNETSECURITY

SUBSCRIBE



Bridging the “front and back of the house”: A lesson in risk management

John Milburn

CEO, Clear Skye

Between cloud proliferation, new tech infrastructure and tools and an increasingly distributed workforce, organizations are struggling to implement proper risk management practices. They often ignore one of the most important components of a solid risk management strategy: efficient communication between the “front and back of the house.”

How can it be done?

A successful risk management program involves key business stakeholders — the “front of the house” — defining policies around risk and subsequent consequences of not adhering to them. Once established, these policies are then disseminated to the various functional or system owners — the “back of the house” — who are then tasked with implementing them for their departments or teams.

Historically, there's been big variances in how functional leaders incorporate these policies, monitor them, and report on their success.

Artificial intelligence (AI)-backed automation tools can be extremely useful for streamlining risk and compliance but, if technology is not vetted thoroughly, throwing it at the problem can cause even bigger issues down the line. But the problem has never been the lack of appropriate tooling - rather, the issue lies in organizational silos that keep these tools and initiatives from functioning together.

> *By consolidating risk management strategy and real time monitoring and measurement in one place, you get less context-switching, reduced friction, and increased efficiency.*

This disconnect is prevalent, which is why we're seeing more businesses look for solutions that bridge the "front and back of the house" within the same workflow. By consolidating risk management strategy and real time monitoring and measurement in one place, you get less context-switching, reduced friction, and increased efficiency. Policies and expectations of how to follow them are streamlined throughout an entire organization, making it easy to follow and ensuring risk management efforts aren't in vain.

The sentiment is easy to understand, but implementation typically comes with more challenges. So, how do enterprises get ahead of the curve before the headaches of new tech integrations or worse? There are several ways to attack this, but the easiest and most impactful is to prioritize solutions that work seamlessly with your existing technology stack. This is sometimes referred to as a platform-native approach, and it serves as the proverbial bridge within an organization.

Conventional knowledge has led companies to default to best-of-breed solutions to fix their technological woes. But this approach requires extra due diligence to ensure they complement existing systems and are accompanied with appropriate training for employees who need to get comfortable with new tech interfaces and processes. In other words, a lot needs to go right for individual solutions to get off the ground successfully. A platform-native approach — if done right — will achieve these things without anyone even knowing it's there.

A platform-native approach

Seamless application integration synonymous with a platform-native approach takes a lot of disparate capabilities and makes sure they work together. In the case of risk management, it does this by making sure all systems and people have the correct access and permissions organization-wide. Access to sensitive information is restricted only to those that need it, compliance is automated, and auditing is performed with a press of a button, instead of being a drawn-out, manual IT effort.

When you consider the nature of today's hybrid and remote working environments, streamlining risk management and compliance becomes even more important. Most organizations have added new applications and technologies to power pandemic-driven work needs. All these systems require an added layer of security and access. Combine this with what's being called "The Great Resignation" - employees leaving their jobs at an unprecedented rate - and provisioning and deprovisioning individual access to company information and systems might as well be a full-time job.

How many of us have left a job only to use our former company logins to access systems or information we've left behind? In many cases, this is innocent — we forgot to save a colleague's email or need access to an old document saved on the company server. But it also leaves organizational data vulnerable — financials, customer information, trade secrets — that could cause a world of hurt if it falls into the wrong hands.

In another instance, a new employee may need a company mobile phone or laptop provisioned. Normally, you would put in a ticket into IT and they would evaluate entitlements on an individual basis. But this doesn't take into account roles and responsibilities across multiple business applications, which can have cascading consequences in other places.

A platform-native approach automates these constantly changing, hard-to-keep-track-of permissions, putting risk and compliance at the center of your business. Beyond better privacy and security measures, this offers another major benefit to business: increased time-to-value and productivity. With less energy spent on IT downtime and hurdles with new tech adoption, employees can focus on their jobs and making real contributions to the business, rather than deal with the growing pains of learning new systems or not having access to what they need.

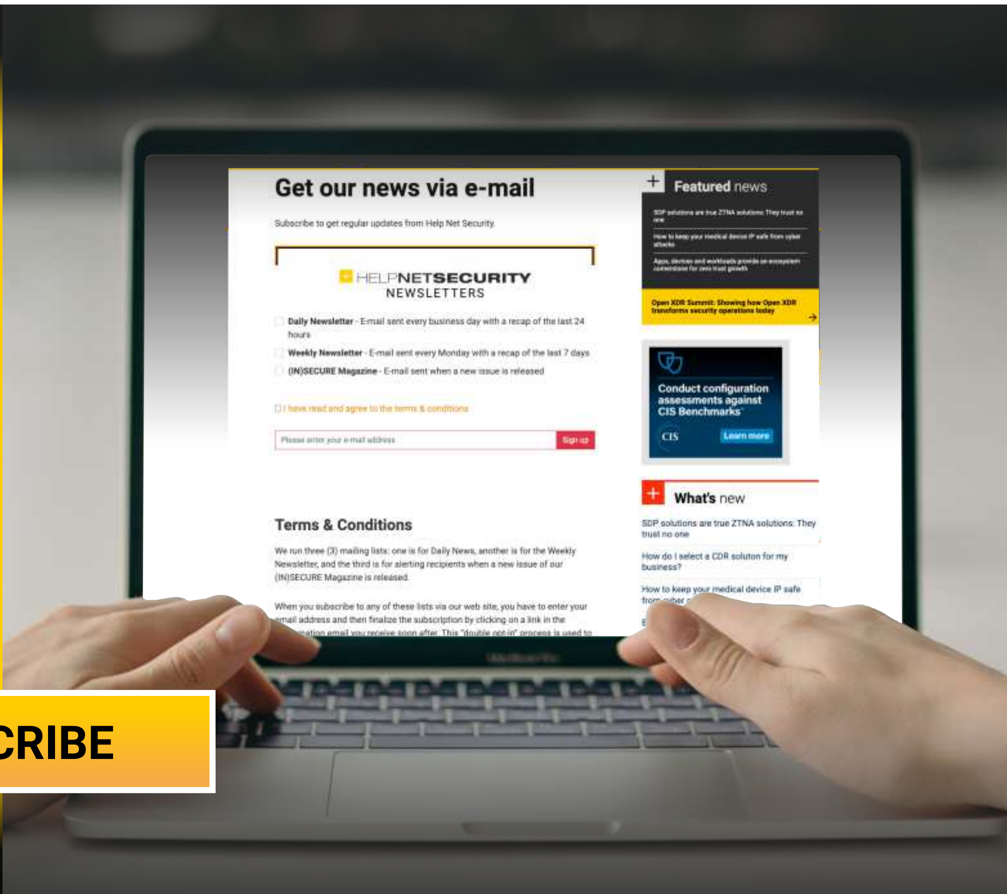
A company can invest in all the best-of-breed solutions under the sun, but if there's nothing bridging the people to new technology and processes, there's no real ROI to be gained. Connecting the "front and the back of the house" is critical to risk management, and a platform-native solution is one of the most effective ways to achieve this for all business systems.

A company can invest in all the best-of-breed solutions under the sun, but if there's nothing bridging the people to new technology and processes, there's no real ROI to be gained.

HELP NET SECURITY DAILY NEWSLETTER

E-mail sent every business day with a recap of the last 24 hours

SUBSCRIBE



Get our news via e-mail

Subscribe to get regular updates from Help Net Security.

HELPNETSECURITY NEWSLETTERS

□ **Daily Newsletter** - E-mail sent every business day with a recap of the last 24 hours

□ **Weekly Newsletter** - E-mail sent every Monday with a recap of the last 7 days

□ **(IN)SECURE Magazine** - E-mail sent when a new issue is released

□ I have read and agree to the terms & conditions

Please enter your e-mail address | Sign up

Terms & Conditions

We run three (3) mailing lists: one is for Daily News, another is for the Weekly Newsletter, and the third is for alerting recipients when a new issue of our (IN)SECURE Magazine is released.

When you subscribe to any of these lists via our web site, you have to enter your email address and then finalize the subscription by clicking on a link in the confirmation email you receive soon after. This "double opt-in" process is used to

Featured news

SDP solutions are true ZTNA solutions: They trust no one

How to keep your medical device IP safe from cyber attacks

Apps, devices and workloads provide an ecosystem cornerstone for zero trust growth

Open XDR Summit: Showing how Open XDR transforms security operations today

Conduct configuration assessments against CIS Benchmarks

CIS Learn more

What's new

SDP solutions are true ZTNA solutions: They trust no one

How do I select a CDR soluton for my business?

How to keep your medical device IP safe from cyber

Why security strategies need a new perspective

Darren Fields

VP of Cloud Networking EMEA, Citrix

After a stream of ransomware campaigns, data leaks, and attacks on critical infrastructure, businesses understand their digitization strategy needs to be complemented by a well-designed cybersecurity strategy. But, confronted with a complex and confusing threat landscape and an equally multi-faceted security vendor landscape, many are uncertain what their security strategy should look like.

In the current debate, one essential factor is often overlooked: the people most relevant for your security strategy may not even work for your company yet (and no, I'm not talking about those incredibly hard-to-find security professionals.)

Many cybersecurity discussions focus on specific threats: ransomware, intellectual property theft, or any of the numerous digital holes allowing threat actors to break into company networks and wreak havoc.

A second, equally prevalent strand of debate focuses on individual components of the environment that need protection: a company's business-critical core applications, its email and collaboration infrastructure, the cloud services it uses, its website and e-commerce applications, or – in the manufacturing industry – the increasingly internet-connected manufacturing plants with their often insufficient mechanisms for securing operational technology (OT) infrastructure.

A third aspect tends to come into play only as an afterthought: the employees. When they are mentioned in the security debate, it tends to be either as targets for social engineering campaigns, as "dumb users" clicking on malicious links that open doors for threat actors, or as malevolent insiders exfiltrating sensitive data. Rarely, however, are employees given the full weight they deserve in security discussions: the pivotal role around which all other aspects need to revolve. It is employees, after all, who work with all these business-critical applications and sensitive data pools, and they are the people who drive every company's business. In security strategies, employees need to take center stage, instead of being relegated to the wings.

> *In security strategies, employees need to take center stage, instead of being relegated to the wings.*

When it comes to designing a cybersecurity strategy, it makes sense to move beyond all the noise about the latest and most sophisticated attacks and the latest and most sophisticated security solutions, and focus attention on the employees instead – but not necessarily on the current staff. Rather, the fundamental security strategy question is: what will the needs and the security requirements of my employees be in four years' time?

> *The latest generations of digital workers have long progressed to using mobile, sometimes even privately-owned devices to access a steadily growing range of cloud services, in addition to corporate resources, from anywhere.*

The workforce of 2026 will be digital - much more digital than today's - even in areas that traditionally have been considered less prone to digitization, such as workers on factory floors, in communal services, or in agriculture. At the same time, employees already working digitally today will most likely not be the office workers that used to dominate many business campuses in pre-COVID lockdown times. The reason for that is that even before the pandemic, digital work had shifted towards flexible hybrid work.

The latest generations of digital workers have long progressed to using mobile, sometimes even privately-owned devices to access a steadily growing range of cloud services, in addition to corporate resources, from anywhere. The pandemic, with its recurring lockdowns across many countries, has simply accelerated this trend, and has made it more obvious to the public.

The digital workforce – especially the highly skilled professionals that businesses compete for in the global "war for talent" – will increasingly insist on being able to work efficiently, but at the same time conveniently and securely, wherever they want or need to engage. Some will bring their own devices, some will prefer to use corporate-owned ones, and some will use a mix of both. At the same time, the move towards cloud services is bound to intensify, while many businesses (e.g., manufacturing) will also continue to deploy a growing number of applications at the edge of their networks. This will result in a progressively complex hybrid application landscape consisting of on-premises legacy technologies, modern on-premises or cloud-based applications, mobile apps, and a dynamic set of cloud services. Here, the challenge will not only be to protect employees in working with this elaborate mix of applications and services – it will also mean keeping use of unwanted apps and services at bay, or at least monitoring it closely.

Taking the work, collaboration, and usability needs of their future workforce as a reference point, decision makers can evaluate: What will be the most likely – and most critical – security risks for this workforce? For example, high-profile employees will sooner or later find themselves in the crosshairs of targeted attacks, be it by cybercriminals or state-backed threat actors. At the same time, it is important to remember that basically every employee, from the call center agent to the HR or finance team, will be targeted – after all, a successful attack hinges on a single person clicking on a malicious link.

What will be the most likely – and most critical – security risks for this workforce?

Once the risk landscape of the future workforce is established, numerous questions follow naturally:

- What will employees' most pressing needs be when it comes to working securely from anywhere, anytime, with any device of their choice, and with their preferred set of apps and services?

- How flexible and scalable will the security architecture need to be to cope with the dynamic nature of the hybrid multi-cloud infrastructure accessed by the distributed workforce?

- Most importantly, how can employees' security needs be balanced with a smooth user experience – especially considering that complex security tools as well as slow app and data accessibility will entice employees to start looking for workarounds, thereby weakening the company's security posture?

- And how can this security posture be monitored continuously without running the risk of impeding employees' productivity and motivation?

What is now called the "new normal" of flexible remote work will soon be the "well-established normal". The whole digital workforce, not just highly skilled individuals, will expect to be able to work flexibly, remotely, in accordance with their individual needs, and securely. They will want – and need – to decide for themselves what is best suited to their work style, and to the current task at hand.

The security architecture will have to support the full spectrum of these needs and requirements. Decision makers should plan for the workforce their business will depend upon in the future, not for the problems they battle today – even if that means planning for the security of employees they don't even have yet.

The whole digital workforce, not just highly skilled individuals, will expect to be able to work flexibly, remotely, in accordance with their individual needs, and securely.

Industry news

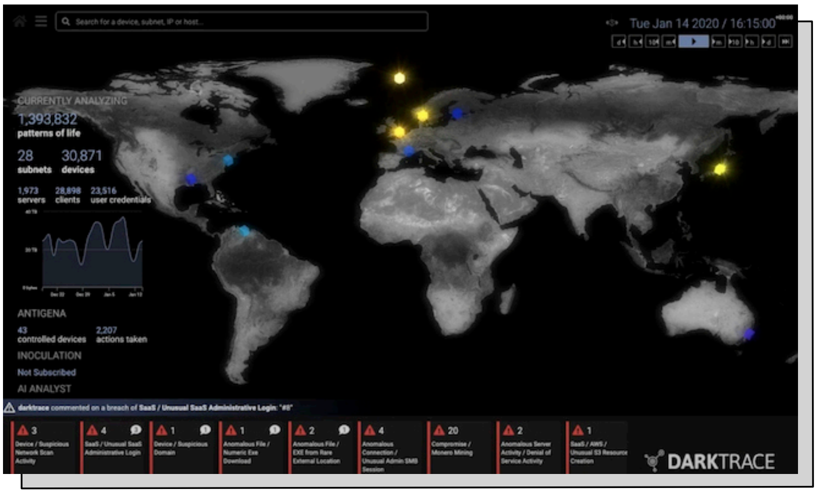
Darktrace adds open investigations to Cyber AI Analyst platform

Darktrace announced significant enhancements to its Cyber AI Analyst product as it now groups incidents to encompass the life cycle of complex compromises as they develop and progress across various entities within a business's digital estate.

With ever-expanding, unique digital estates, it's mission-critical that Cyber AI Analyst investigations remain bespoke to their environment rather than follow a one-size-fits-all model with pre-programmed investigation tactics. AI Analyst's on-the-fly technical approach to investigations enables it to find the needle in a thousand haystacks that might be the key evidence to connecting disparate compromises.

Historically, multiple incidents would have remained separate. Now, AI Analyst can automatically merge incidents when it discovers a link connecting them. This shift to open investigations has early adopter customers experiencing up to a 63% reduction in total incidents and up to a 92% reduction in the most critical incidents, further decreasing time-to-meaning and analyst triage time, enabling customers to spend more time focusing on macro-level tasks and initiatives.

In addition to continuously running based on directly observed events, Cyber AI Analyst open investigations can be run manually by a human member of the security team or be triggered automatically by a third-party event, perhaps by an alert ingested directly from another security solution to validate and further contextualize their detections and decisions.



darktrace commented on a breach of SaaS / Unusual SaaS Administrative Login: "#8"

Search for a device, subnet, IP or host...
Tue Jan 14 2020 / 16:15:00
CURRENTLY ANALYZING
1,393,832
patterns of life
28
subnets
30,871
devices
1,973
servers
28,898
clients
23,516
user credentials
ANTIGENA
43
controlled devices
2,207
actions taken
INOCULATION
Not Subscribed
AI ANALYST
3 Device / Suspicious Network Scan Activity
4 SaaS / Unusual SaaS Administrative Login
1 Device / Suspicious Domain
1 Anomalous File / Numeric Exe Download
2 Anomalous File / EXE from Rare External Location
4 Anomalous Connection / Unusual Admin SMB Session
20 Compromise / Monero Mining
2 Anomalous Server Activity / Denial of Service Activity
1 SaaS / AWS / Unusual S3 Resource Creation
DARKTRACE

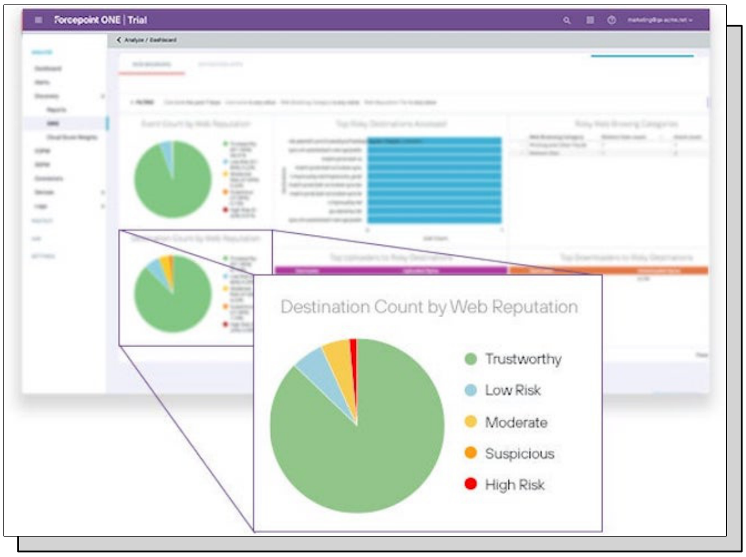
Forcepoint ONE protects sensitive data across business applications and BYOD devices

Forcepoint launched Forcepoint ONE, an all-in-one cloud platform that simplifies security for both traditional and remote workforces, allowing users to gain safe, controlled access to business information on the web, in the cloud and in private applications.

Forcepoint ONE makes it easy for customers and partners to adopt Security Service Edge (SSE) by unifying crucial security services including Secure Web Gateway (SWG), Remote Browser Isolation (RBI), Content Disarm and Reconstruction (CDR), Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA). Integrated Advanced Threat Protection (ATP) and Data Loss Prevention (DLP) also keeps malware out and protects sensitive data across business applications and BYOD devices, eliminating the need for fragmented products.

With Forcepoint ONE, security teams can now manage a single set of policies across all apps, from one cloud-based console, through one endpoint agent, with agentless support for unmanaged devices.

Simplifying security can be a daunting task because users can work from anywhere, browse high-risk websites and connect to unmanaged SaaS apps from unmanaged devices. Forcepoint's all-in-one approach allows one security policy to enforce rules and prevent unauthorized information access or sharing.



Anomali XDR solution helps enterprises against advanced cyber threats

Anomali launched a cloud-native XDR solution built on the Anomali Platform, providing customers with visibility across all security telemetry from endpoints to the public cloud.

The Anomali Platform is fueled by big data management, machine learning, and the world's largest repository of global intelligence. Because Anomali enables easy integration with existing security infrastructures, Business Leaders, CIOs and CISOs can optimize their overall security investments and create more efficient and effective detection and response capabilities ultimately to proactively stop today's escalating advanced cyber threats, including ransomware.

Redstor launches a service for IT service providers to protect Kubernetes environments in AWS

Redstor launched a new service aimed at transforming how managed and cloud service providers (MSPs and CSPs) protect Kubernetes environments in AWS.

By adding support for Amazon Elastic Kubernetes (Amazon EKS), a managed container service for handling applications in the cloud or on-premise, Redstor partners can eliminate complex scripting and scale customer backups simply and rapidly.

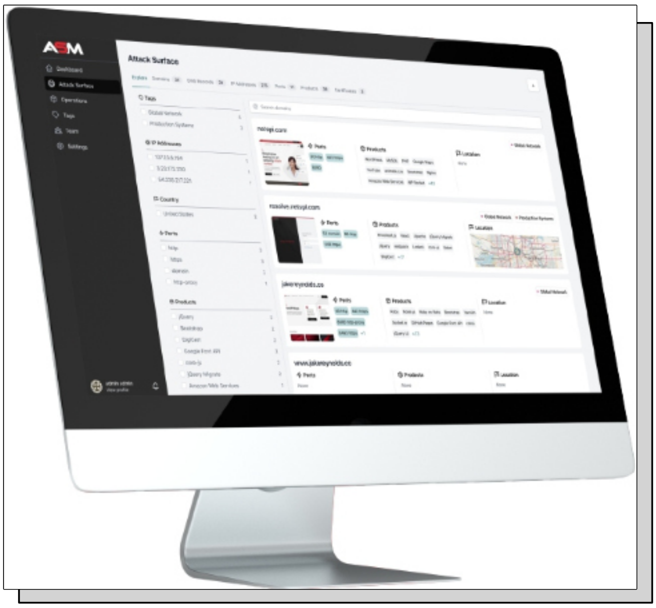
Redstor's smart data management platform allows IT administrators of all levels – not just Kubernetes experts – to protect and recover data in minutes, including within clusters. Traditional, machine-based backups were not designed for modern, container-based applications. To recover these quickly, service providers previously had to deploy a separate Kubernetes solution to backup not only applications, but configurations, as well.

NetSPI Attack Surface Management enhances security posture for organizations

NetSPI introduced Attack Surface Management to help secure the expanding, global attack surface. The platform delivers continuous pentesting backed by NetSPI's global security testing team to help organizations inventory known and unknown internet-facing assets, identify exposures, and prioritize critical risks to their business.

Attack Surface Management is a core component of NetSPI's Penetration Testing as a Service (PTaaS) delivery model. It complements the company's established Penetration Testing and Adversary Simulation technology-powered services to provide a full suite of offensive security solutions for its customers.

The Attack Surface Management (ASM) platform also features simple set-up, tracking and trending data over time, asset intelligence, Slack and email integrations, open source intelligence gathering, asset and exposure prioritization, port discovery, and more.



Armorblox Advanced Data Loss Prevention protects critical business workflows

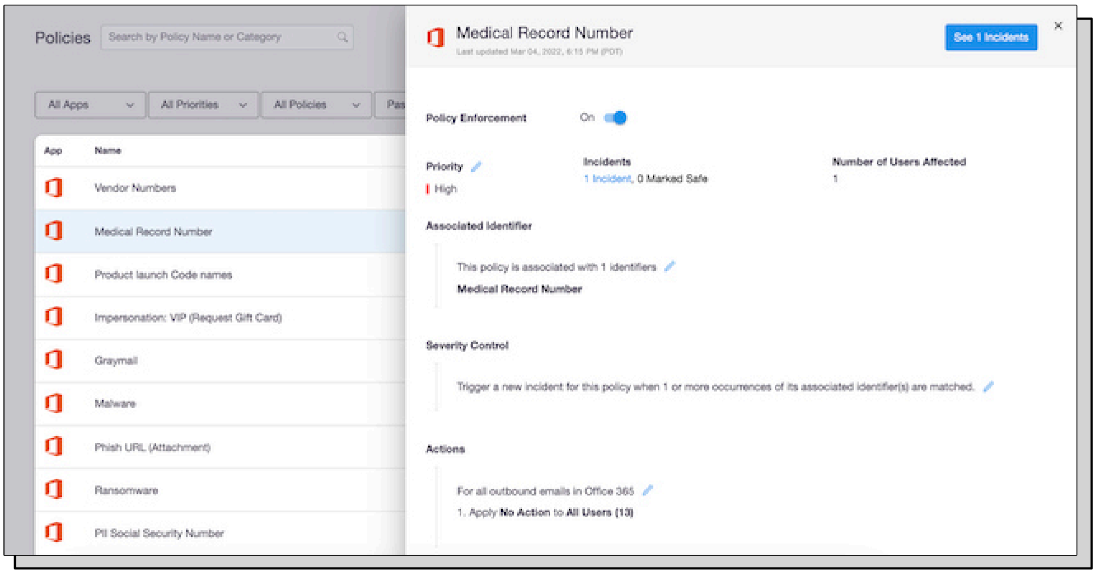
Armorblox announced the addition of Advanced Data Loss Prevention to its cloud-delivered email security platform.

With this new service, Armorblox becomes the first vendor to bring natural language understanding (NLU) to prevent data loss in Microsoft Office 365, Microsoft Exchange, and Google Workspace environments. When comparing the new DLP service with NLU to legacy solutions based on static rules and regexes, false positives are reduced by a factor of 10.

The Armorblox Advanced Data Loss Prevention service offers a NLU-based analysis of email content and attachments to detect and safeguard critical business workflows, including invoices, payroll data, wire transfer requests, medical records, and legal documents. Combining insights from business operations with content, context, user, and behavior analytics, Armorblox helps to prevent sensitive data from leaving the organization. Powered by NLU and artificial intelligence (AI), Armorblox's enriched insights bring deeper understanding and context to data, resulting in prevention capabilities not possible through traditional approaches.

Armorblox Advanced Data Loss Prevention protects organizations against accidental and malicious leaks of sensitive data. With email-based phishing attacks accounting for 90% of data breaches, Armorblox Advanced Data Loss Prevention is best positioned to help organizations limit the financial impact caused by targeted email attacks, malicious insider actors, or socially engineered threats.

Importantly, Armorblox's autonomous policy engine removes the need for manual configuration and ongoing management of all email DLP security policies, which are created and delivered out of the box. Using the NLU engine, DLP policies are constantly updated based on global learnings, helping organizations avoid any ongoing manual intervention to keep the policies current and accurate.



App	Name
	Vendor Numbers
	Medical Record Number
	Product launch Code names
	Impersonation: VIP (Request Gift Card)
	Graymail
	Malware
	Phish URL (Attachment)
	Ransomware
	PII Social Security Number

Medical Record Number
Last updated Mar 04, 2022, 6:15 PM (PDT)

Policy Enforcement On

Priority: High

Incidents: 1 Incident, 0 Marked Safe

Number of Users Affected: 1

Associated Identifier

This policy is associated with 1 identifiers
Medical Record Number

Severity Control

Trigger a new incident for this policy when 1 or more occurrences of its associated identifier(s) are matched.

Actions

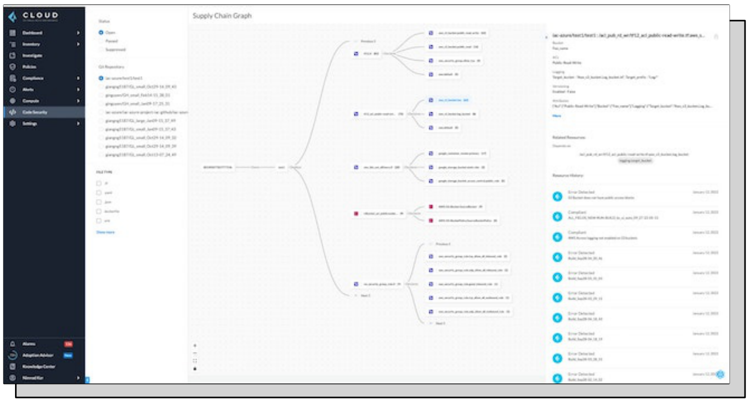
For all outbound emails in Office 365
1. Apply **No Action** to **All Users (13)**

Palo Alto Networks unveils Prisma Cloud Supply Chain Security to reduce code complexity and risk

With software supply chain attacks rising rapidly, Palo Alto Networks announced Prisma Cloud Supply Chain Security to provide a complete view of where potential vulnerabilities or misconfigurations exist in the software supply chain — allowing organizations to quickly trace to the source and fix them.

If not quickly fixed or, better yet, avoided during coding, these security flaws could allow attackers to infiltrate systems, spread malicious payloads throughout an organization's software and access sensitive data.

Prisma Cloud Supply Chain Security helps provide a full stack, full lifecycle approach to securing the interconnected components that make up and deliver cloud native applications. It can help to identify vulnerabilities and misconfigurations in code, including open source packages, infrastructure as code (IaC) files and delivery pipelines, such as version control system (VCS) and CI pipeline configurations.



AvePoint Ransomware Detection identifies suspicious behavior within users' Microsoft OneDrive

AvePoint launched Ransomware Detection, as part of Cloud Backup for Microsoft 365, to further protect digital collaboration data.

This new capability proactively detects suspicious behavior within users' Microsoft OneDrive, while minimizing disruption to productivity and collaboration. After detecting unusual activity, Cloud Backup provides detailed reports to shorten the investigation and flag the areas of question for Customer's Admin, and if necessary, restores all or specific OneDrive data, recovering business-critical information quickly for Cloud Backup customers.

AvePoint is also launching its Ransomware Warranty for MSPs, which primarily serve small business clients via its global distribution network, to give the ultimate assurance they will be protected. It provides coverage of up to one million dollars if customer data is not recovered due solely to a failure of these eligible products: AvePoint Cloud Backup for Microsoft 365, Dynamics 365, Google Workspace and Salesforce. Detailed terms and conditions apply.

Sumo Logic Cloud SOAR enhancements increase automation for security teams

Sumo Logic announced new offerings further advancing its Sumo Logic Cloud SOAR with the War Room and App Central features.

The War Room provides security teams with the details of an incident to expedite manual processes that could typically take minutes to now close within a matter of seconds. Within App Central, critical resources, including use cases, integrations, and playbooks, are brought together to boost necessary automation so that security teams can build standard operating procedures and respond faster to incidents.

The Sumo Logic Cloud SOAR War Room and App Central add efficiency and even more automation to drive the most important Security Operations activities.

Imperva API Security protects data across legacy and cloud-native applications

Imperva introduces Imperva API Security with continuous API discovery and data classification. The product is deployed easily in any environment to provide visibility and protection of data across legacy and cloud-native applications.

As a service offering, it can be seamlessly enabled by Imperva Cloud Web Application Firewall (WAF) customers or quickly deployed as a standalone to gain visibility into all API traffic.

Imperva API Security provides protection for Application Programming Interfaces (APIs) in developer environments that often lack adequate security controls and are vulnerable to malicious or inadvertent exposure.

Imperva API Security enables rapid, secure development by providing continuous visibility and protection for all APIs. The product mitigates the risk of data breaches and data leakage by uncovering shadow APIs, and suggests remediation for software developers and security administrators.

Imperva API Security is a product designed to benefit both the security and development teams. As a core component of the Imperva Web Application & API Protection platform, customers can protect critical applications and infrastructure from online fraud, DDoS attacks, and API abuses.

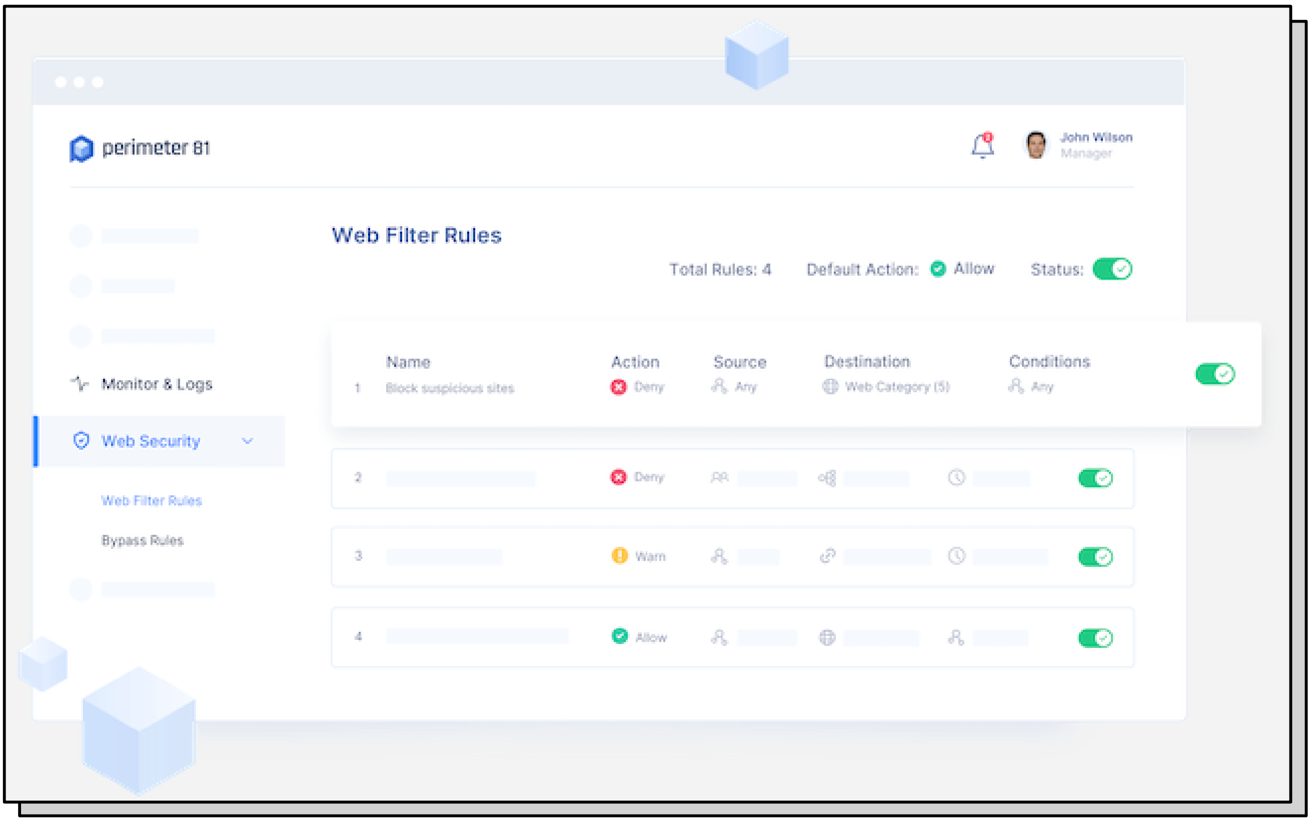
Perimeter 81 Secure Web Gateway blocks access to specific URLs or categories of websites

Perimeter 81 has added a Secure Web Gateway component to its Security Services Edge (SSE) solution.

The Secure Web Gateway (SWG) is extending the company's signature ease of use to Web filtering and ensures that company employees are safe from malicious websites and unsafe content, no matter where they are working.

Perimeter 81's Secure Web Gateway will block access to specific URLs or categories of websites based on the user or the user's role and other conditions such as the day of the week. These categories are dynamically updated daily so that no site flies under the radar.

Employee access to "blocked" or "warned" websites is tracked and logged for monitoring and compliance with auditing requirements and company policies. Bypass rules can be created for those programs that do not require SSL inspection and to ensure employee privacy, for example, when visiting financial or healthcare sites.



Web Filter Rules

Total Rules: 4 Default Action: Allow Status:

	Name	Action	Source	Destination	Conditions
1	Block suspicious sites	Deny	Any	Web Category (5)	Any
2		Deny			
3		Warn			
4		Allow			

PACE AP White-Box Works protects financial institutions from sophisticated attacks

PACE AP launched its new, EMVCo certified, White-Box-Works code generator for banks, payment service providers (PSPs), schemes, and other financial institutions.

Unlike traditional solutions, White-Box Works gives the customer complete, independent control over their protected code, ensuring their encryption keys and proprietary algorithms never leave the customer's premises. White-Box Works can transform any C-code into a protected white-box variant in a single step, offering flexibility, security, and efficiency.

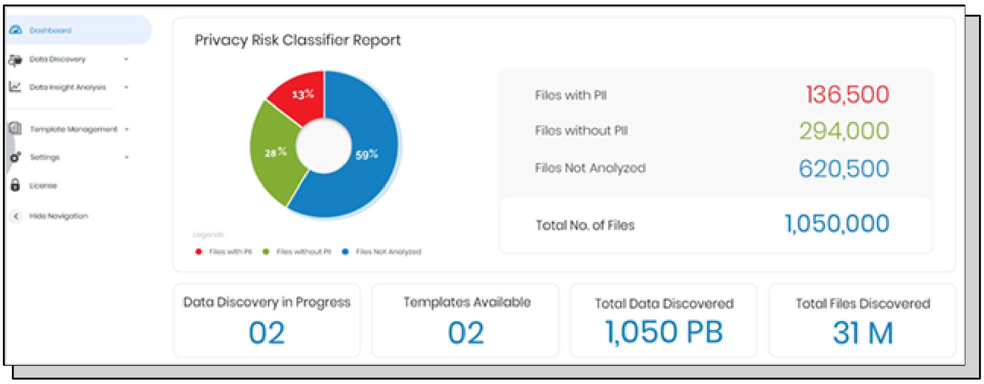
This level of in-house control also promises to increase operational efficiency for the customer, since they are no longer beholden to a white-box library vendor's build schedule and can develop their application in accordance with their internal schedules. It also enables the customer to use, replace and update their deployed encryption keys and algorithms at will, with no need to re-engage PACE Anti-Piracy, or any other third-party vendor, to do so.

Data Dynamic Insight AnalytiX 1.4 reduces data vulnerability for enterprises

Data Dynamic released Insight AnalytiX 1.4, which is focused on enhancing the product's Data Protection and Security Functionalities.

The upgrade includes flexible and scalable data discovery, deep analytics, and reduced data vulnerability to help organizations ensure maximum accuracy in PII/sensitive data discovery and an upgraded remediation functionality.

The new features in Insight AnalytiX 1.4 make it an excellent application for risk identification and remediation. The latest version of Insight AnalytiX allows users to generate a Data Insight report on a dataset by building advanced multi-level logical expressions and a combination of logical operators. It reduces the chances of missing sensitive personal data, ensuring the highest accuracy in data discovery. The report is powered by deep analytics (both descriptive and diagnostic) to help enterprises get a clear understanding of the risk that exists and an easy means of quantifying it.



Privacy Risk Classifier Report

Files with PII	136,500
Files without PII	294,000
Files Not Analyzed	620,500
Total No. of Files	1,050,000

Data Discovery in Progress	Templates Available	Total Data Discovered	Total Files Discovered
02	02	1,050 PB	31 M

The four types of remote workers your security awareness program must address

Ben Smith

Field CTO, NetWitness

No matter how much technology you acquire or how many specific technical controls you install, when it comes to your information security awareness program, the most important control to tune within your environment is your people.

I'm not telling you anything new here. But as we move into a third year of employees either working regularly from home or coming back into an environment which may be dramatically reconfigured and is staffed differently than before (the office), we are not going back to the way things were in "the before times".

It's important that your current security awareness efforts are appropriate for how your employees work today, not how they worked two years ago.

It's important that your current security awareness efforts are appropriate for how your employees work today, not how they worked two years ago.

Here are four employee personas for you to consider and recognize as you review and update your security awareness program:

- **Employees as first-line defenders.** The strongest security cultures are those where each employee fully understands that they are on the front lines. They are extended members of and the early warning system for your core team in the SOC.

Make it easy for them to express concern about something they've seen or experienced. It's the same mindset of the "If you see something, say something" mantra we all see when we take public transportation.

Don't settle for developing and publishing an overly complicated policy which details the many steps the employee should follow if they believe there is suspicious activity. There's often too much friction.

An employee who finds it too hard to fill out your helpdesk form to open a ticket may be an employee who decides it's just not worth it.

Think instead about how that concerned employee can quickly reach your information security team directly via a phone call and via chat. Providing multiple channels to ask for help increases the chances that one of them will be used. An employee who finds it too hard to fill out your helpdesk form to open a ticket may be an employee who decides it's just not worth it.

- **Employees as people.** And people are not machines. We get distracted. We get tired. We make mistakes. We want to do the right thing for our organization, and we need to get our job done, but sometimes it can seem like both goals are in opposition to one another.

When your training curriculum is presented like most other trainings employees consume – sitting through a multiple-choice exercise, trying to hit the minimum passing score to just to get it out of the way – you run the risk of your audience tuning out.

We want to do the right thing for our organization, and we need to get our job done, but sometimes it can seem like both goals are in opposition to one another.

Consider a continuous "drip" approach versus a once-a-year "hammer" approach. One way to accomplish this is to wrap additional content around the main curriculum/test each year – in some organizations, the wrapper might even replace the single test.

One example: a quarterly email which directly connects a reported incident elsewhere in the industry to the employee behavior which led to the incident.

Taking a more overt approach where you explicitly nudge employees during their day-to-day work is another alternative: you may have technology in place which can monitor email during composition and insert a "are you sure?" prompt when an email is going outside the organization to a known-risky domain, or if it contains an attachment with sensitive information.

- **Employees as parents.** Employees with families have found the last two years especially challenging. They didn't sign up to do their own tech support at home. They didn't sign up to enforce your corporate-grade security rules within their home environment. And they didn't sign up for sometimes unusual working hours and significantly increased stress when trying to be a worker and a parent during a pandemic, when those two roles are sitting behind the very same laptop on the dining room table.

Help them, show them how to secure their work devices and their home devices. Don't be afraid to explain the "why" along with the "how."

As an example, maybe you sent out explicit guidance about home networks: "Make sure your Wi-Fi router's password is complex." Good advice, to be sure. But from the employee's perspective, what exactly is a complex password? Why is it that a complex password does a better job protecting an information asset versus a non-complex password? Where can a non-technical employee check to see what the current Wi-Fi password is? Is there a difference between an administrative password and the password they use to join a device to their Wi-Fi network? How do they recognize the distinction between their Wi-Fi router and their cable modem? Issue your guidance but take the time and the care to explain.

Why is it that a complex password does a better job protecting an information asset versus a non-complex password?

- **Employees as threats.** We know that there are two primary types of threats from our employee population: accidental, and intentional. Your security awareness content should account for these two audiences.

Trainings should include scenarios involving both external and internal threat actors, scenarios which are more than "don't do this" but "if you see this, here's what to do." This can also be a good opportunity to explain exactly why your organization reserves the right to monitor employees. And even in environments where you may be less concerned about insider risk, ensure that your training also includes a third-party angle, especially for that subset of your team who works with external partners.

Trainings should include scenarios involving both external and internal threat actors, scenarios which are more than "don't do this" but "if you see this, here's what to do."

There will always be employees who just don't care, who won't care, and can't be bothered to pay attention to your training curriculum. Your job is to reach as much of your audience as you can, and to recognize that outliers will always exist.

Remember: work is not a location, but an outcome. Now is the right time to review your existing security awareness program to confirm it respects the new reality your remote employees are experiencing every day.

There will always be employees who just don't care, who won't care, and can't be bothered to pay attention to your training curriculum. Your job is to reach as much of your audience as you can, and to recognize that outliers will always exist.

Reducing the blast radius of credential theft

Tony Cole

CTO, Attivo Networks

Application Programming Interfaces (APIs) underpin today's digital ecosystem as the essential connective tissue that allows companies to exchange data and information quickly and securely. As the post-pandemic world leans heavily on digital interaction to maintain user connections, the volume of API traffic has grown rapidly. However, this growth has also brought on emerging security challenges.

While traditional application security controls remain necessary, they are not quite up to the API security challenge. Fortunately, there are certain basic API security practices organizations can implement to create a more resilient API security posture.

What is threatening API security?

When contemplating API security, you must consider its risks and exposures. Hackers spend more time poking at APIs than most companies do maintaining them. It is rare to see an attacker "break" an API. Rather, the most common threat vector is misconfigurations and weak links between APIs deployed in each piece of software.

> *Hackers spend more time poking at APIs than most companies do maintaining them.*

The first step in fixing the API security problem isn't necessarily a new testing solution, but rather taking stock of how many APIs an organization has deployed and how they are interacting with one another. Each API is unique and needs individual attention and detailed understanding. Without visibility into the nature and scope of its API deployments, an organization will find itself hamstrung at the earliest stage in attempting to tackle its API security risk.

Another challenge facing security practitioners when implementing API security programs are unclear roles and responsibilities for security teams. This commonly cited issue means that there are gaps in API maintenance, monitoring and security, and they become doorways for hackers to come in. Teams need to be given specific responsibilities regarding API security maintenance to ensure that nuanced differences between APIs are addressed.

What can companies do to ensure they are prioritizing API security?

The original security problems stemmed from a misunderstanding of an API's software-to-software communication. With organizations often having hundreds or even thousands of APIs in use, the task of securing them all is highly complex. The challenge requires a strategic approach for security assessment that can be applied universally and efficiently across a diverse set of APIs.

One example of this type of strategy is D.A.R.T., which stands for Discover, Analyze, Remediate, and Test.

D.A.R.T. serves as both a lens to view security challenges, as well as a litmus test to measure the effectiveness of security efforts and solutions. This solution addresses security across the API ecosystem, from code to production, and needs to be used for each API's unique individual requirements.

- **Discover:** This encompasses the ability to find and inventory all APIs. Enterprises manage thousands of APIs, and many of them are not routed through a proxy or API gateway. APIs that are not routed are not monitored, are rarely audited, and are most vulnerable to mistakes which lead to attacks. It is important to create a complete API inventory enabling the team to discover and assess every API, including legacy and shadow APIs with data classification.

- **Analyze:** The ability to detect API anomalies, changes and misconfigurations is vital. It's important for enterprises to analyze API access, usage, and behavior. Leveraging AI and ML for automated behavior analysis helps to identify issues in real-time. When considering existing detection capabilities or those of an API security vendor, companies must remember they will only be as effective as their ability to discover a complete inventory of APIs.

- **Remediate:** The next step is to have the ability to resolve detected anomalies and misconfigurations. Based on that inventory, teams can begin remediation by identifying misconfigurations and vulnerabilities in the source code, network configuration and policy. Teams can focus on security interventions in the highest-risk areas and provide an effective detection and response. The implementation of automated and semi-automated blocking and remediation of threats means that they can be blocked from even happening.

- **Test:** Even if a detection and response system is implemented, it is important to have continuous testing of the different API endpoints to identify API risks before they emerge. Analyzing APIs and remediating issues while in development allows companies to deploy APIs with complete confidence and trust.

The road ahead

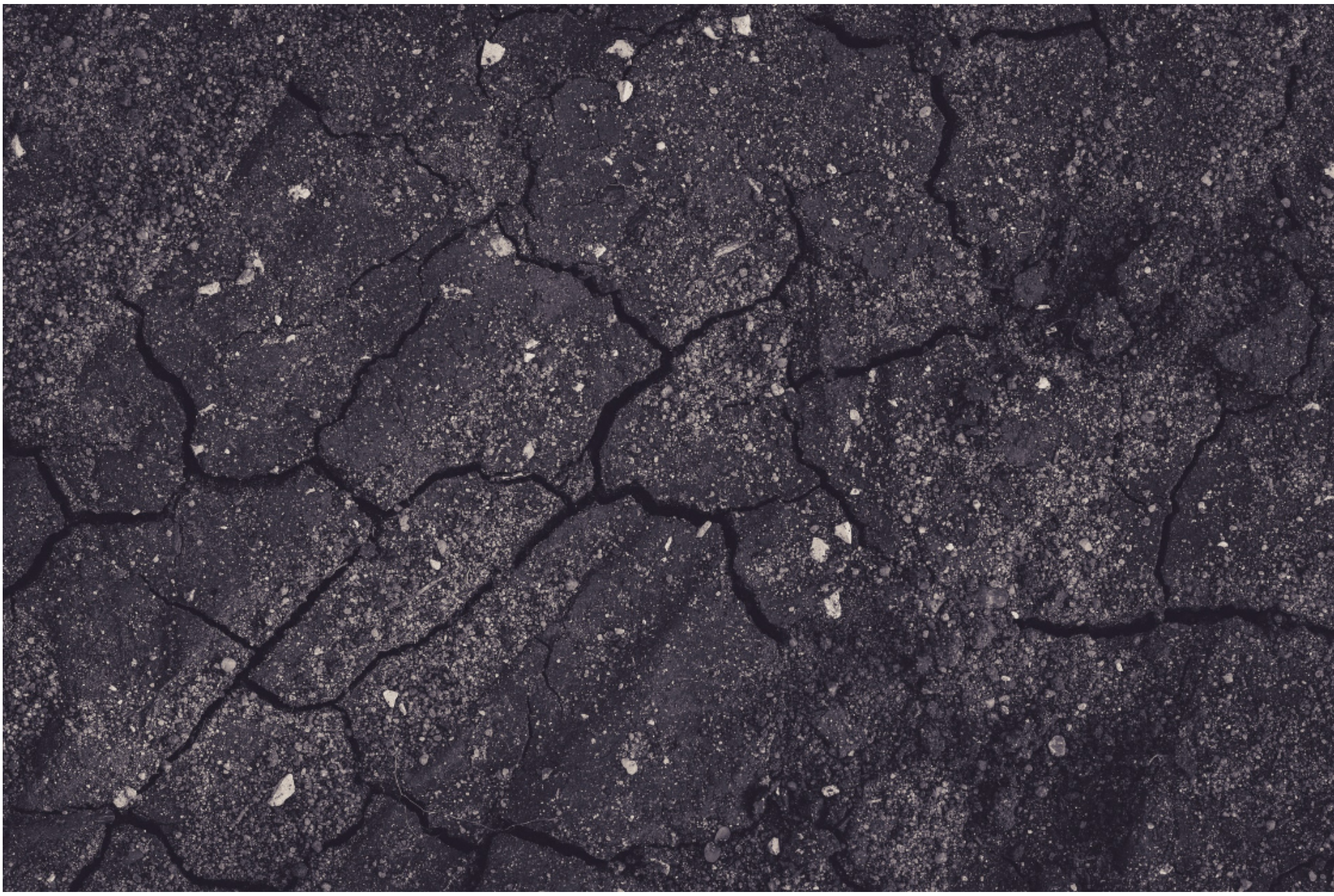
2022 will be the year of the API security "arms race," as security teams and hackers alike bring more sophisticated technologies to the playing field.

Hackers are increasingly turning their attention towards APIs as an attack vector and will undoubtedly develop more advanced tools and methods for exploitation. Hackers have shown that they have and will continue to batter down the doors of companies through their insecure APIs.

Security teams that are too reliant on tools, have unclear roles and responsibilities and do not execute routine API maintenance may be doing their organizations more harm than good.

Taking the time to get educated on specific strategies such as D.A.R.T, ensures that each API is properly managed and secured.

HELPNETSECURITY
HELPNETSECURITY
HEALTHCARE CYBERSECURITY REPORT
Q1 2022
Healthcare Cybersecurity report Q1 2022
FREE DOWNLOAD



Small businesses are most vulnerable to growing cybersecurity threats

Rizwan Virani

President, Alliant Cybersecurity

Many small and medium-sized businesses (SMBs) mistakenly assume (hope?) their size makes them a less appealing target to hackers, without realizing cyber criminals are eager to exploit the unique characteristics that make them even more vulnerable to cyber-attacks.

While protecting digital resources may be easy for large companies that can afford to hire in-house cybersecurity staff and establish threat monitoring and endpoint detection infrastructure, this endeavor can often seem impossible for SMBs. All the while, the dangers for smaller businesses could not be more acute, especially since the businesses' operators and employees are often uninformed about common cybersecurity threats.

By understanding the threats they face and implementing a few relatively low-effort but highly effective protection measures, SMBs can leap into the next phase of growth with their digital assets secured.

Unique threats to SMBs

The scope of cybersecurity threats to small companies is no less varied than the threats large multinational corporations face, but SMBs' size and lack of infrastructure often leaves them more vulnerable to targeted hacking schemes and threats. Hackers often opt for schemes that require less preparation and risk and find easier targets in SMBs.

> *The scope of cybersecurity threats to small companies is no less varied than the threats large multinational corporations face, but SMBs' size and lack of infrastructure often leaves them more vulnerable to targeted hacking schemes and threats.*

One major vulnerability is the disadvantage SMBs face because they often do not control every aspect of their supply chain. A bad actor can conduct a software supply chain hack, isolating smaller vendors and suppliers as weak points with little to no cybersecurity protection, forcing them to unwittingly pass on malware that can disable an entire chain of businesses. SMBs in the logistics and operations industries are particularly vulnerable targets since they are connected to many other companies and will likely be more willing to pay the ransom to quickly resume operations at 100% capacity.

In addition, an entirely new slew of cyber threats has cropped up along with the hybrid work model. In a rush to digitize at the start of the pandemic, many SMBs relied on single systems that they perceived to be safe, including migrating their files and processes to the cloud. They hoped that the cloud's decentralized nature would prevent them from being victimized by cyber attackers. However, even cloud software providers can be infiltrated, as all it takes is one bug to create a vulnerability. Yet most SMBs fail to acknowledge the new vulnerabilities remote work creates and are now even more vulnerable since they are complacently conducting business through unsecured systems.

All these threats represent a growing danger to SMBs' success – and some SMBs are more vulnerable than others. Many of the industries (e.g., agriculture) that never thought they would be targeted and therefore eschewed any type of basic cyber security are years behind in their cyber protection measures.

Regulations add another complication

On top of growing threats, additional cybersecurity compliance requirements and regulations being passed at the state and federal levels are complicating security processes even for those SMBs that want to get serious about cybersecurity.

New state regulations, including the California Consumer Privacy Act (CCPA) and the NY SHIELD Act, broaden the definition of private information and expand data privacy requirements, making it more difficult for SMBs to properly navigate data security compliance since they do not have dedicated staff members to sort through often dizzying regulations.

> *On top of growing threats, additional cybersecurity compliance requirements and regulations being passed at the state and federal levels are complicating security processes even for those SMBs that want to get serious about cybersecurity.*

Getting certified for federal measures like the Cybersecurity Maturity Model Certification (CMMC) will be a boon for any SMB looking to make their bids much more attractive, especially with the flood of new contracts following the passage of the Bipartisan Infrastructure Law. Yet, certification still requires the time-intensive interactions with multiple third-party vendors to successfully navigate this process. Further, many of these requirements have been a moving target in 2021 as businesses have awaited guidance from the Department of Defense regarding the final requirements. These requirements, while important, can overwhelm an SMB already behind on installing cybersecurity protections.

Combatting cyber threats

With all these threats and regulatory requirements swirling around SMBs, operators need to choose the most cost-effective and powerful cybersecurity measures to ensure their data is protected.

> *Implementing cyber hygiene training as part of onboarding and sending out a steady cadence of cybersecurity tips and tricks can help employees understand common phishing schemes and how they might be targeted.*

Arguably the most effective protection measure for SMBs is proper employee cybersecurity education and training, since the weakest aspect of a security system is often the people using it.

Implementing cyber hygiene training as part of onboarding and sending out a steady cadence of cybersecurity tips and tricks can help employees understand common phishing schemes and how they might be targeted. To increase participation, try gamifying trainings or even offering a small incentive for employees who report phishing schemes.

More technical steps include executing routine penetration testing to help organizations understand where their vulnerabilities lie and implementing solutions like multifactor authentication to ensure only verified employees have access to company information.

More involved (but no less important) steps include investing in third-party risk assessment services to formulate a data breach response plan to act quickly if protection measures fail. Ultimately, implementing any one of these solutions will put a company years ahead in terms of data protection.

Cultivating a security-first mindset for software

Onkar Birk

CTO, Alert Logic

There is a “great cyber security awakening” happening across companies. Right now, we need a fundamental new approach to development, so we are not constantly firefighting.

Almost two years into the pandemic, organizations are recognizing that their teams may never be together in one place again. This has pushed a mass adoption of cloud services and SaaS applications to enable their distributed workforces. The pandemic has also fueled an increase in cybercrime, with criminals taking advantage of the chaotic transition to remote work to target vulnerable systems and launch devastating ransomware and supply chain attacks. Understandably, security teams are recalibrating and sorting out where more security investments are needed in the new year.

> *Each time an app is updated with new functionality, there is potential to introduce exploitable vulnerabilities.*

The software development community is responding to these developments and recognizes that approaching security as an afterthought encourages attacks and their resulting damages. Each time an app is updated with new functionality, there is potential to introduce exploitable vulnerabilities.

Vulnerabilities can be introduced in several ways. The pressure to deliver innovative features and get products to market quickly often forces security practices to the wayside, resulting in vulnerable code getting released. The use of pre-built code and components and the idiosyncrasies of the various programming languages can also introduce software vulnerabilities. Even when developers follow secure coding practices, highly motivated cybercriminals are looking for vulnerabilities across a collection of code to be exploited where developers may be working just within a small code subset and not see the bigger picture. In any case, the vulnerability is dealt with through further app updates, which perpetuates the cycle.

Faced with this uphill struggle, app vendors are going to have to ask themselves how they can build security at the level they need into their applications. For many of them, the answer will be to embed what I call "micro-detection" into their apps.

Micro-detection can result in resilient software

Most software today is composed of independent, loosely coupled components that run each app process as a service. These services work and deliver in a standalone capacity, but when they're combined, the whole is far greater than the sum of the parts. Cybersecurity, however, hasn't kept pace with this evolution. It still views the application in totality, making it difficult to effectively mitigate the risks introduced by microservice architecture. Breaking down an application into discrete microservices increases that app's attack surface, as its entry points and communication paths are spread over multiple environments. Cybersecurity's high-level umbrella approach isn't well-suited to detecting and addressing vulnerabilities in these types of modern applications.

Detection is going to have to get down to the micro level to work effectively with microservices. Imagine detection as a set of small service capabilities that can sit and monitor changes within a micro-service. The closer we can get to the source the faster and easier it is to monitor a chain reaction that can lead to an exploit being active. Prevention is great but it's too close to an exploit being active. This may be controversial to some folks, but you need a vaccine to prevent an illness, and the earlier you get it the better you are protected, even if you never come in contact with the virus.

> *The closer we can get to the source the faster and easier it is to monitor a chain reaction that can lead to an exploit being active.*

So, how do you know when to get that vaccine and which one to get? You have to see what's happening and really understand the potential impact. The only sure way to achieve this outcome is for developers to consider how each service they're developing could potentially be exploited and how each exposure would work from one service to the next. Then they'll need to consider the potential for detection capabilities.

This likely means developers will have to identify potential anomalies—a deviation from the baseline in some microservice code, for example—that can provide a "trigger" for detection. A single anomaly in a microservice on its own may be interesting but not particularly important. But when combined with five or six other specific anomalies across the same set of functionalities spanning several microservices, it may indicate something more critical.

Machine learning algorithms could recognize these anomalies as a pattern and flag it for investigation. In this way, developers can build in a series of hooks at the microservice level that could point the way toward a security threat when viewed together.

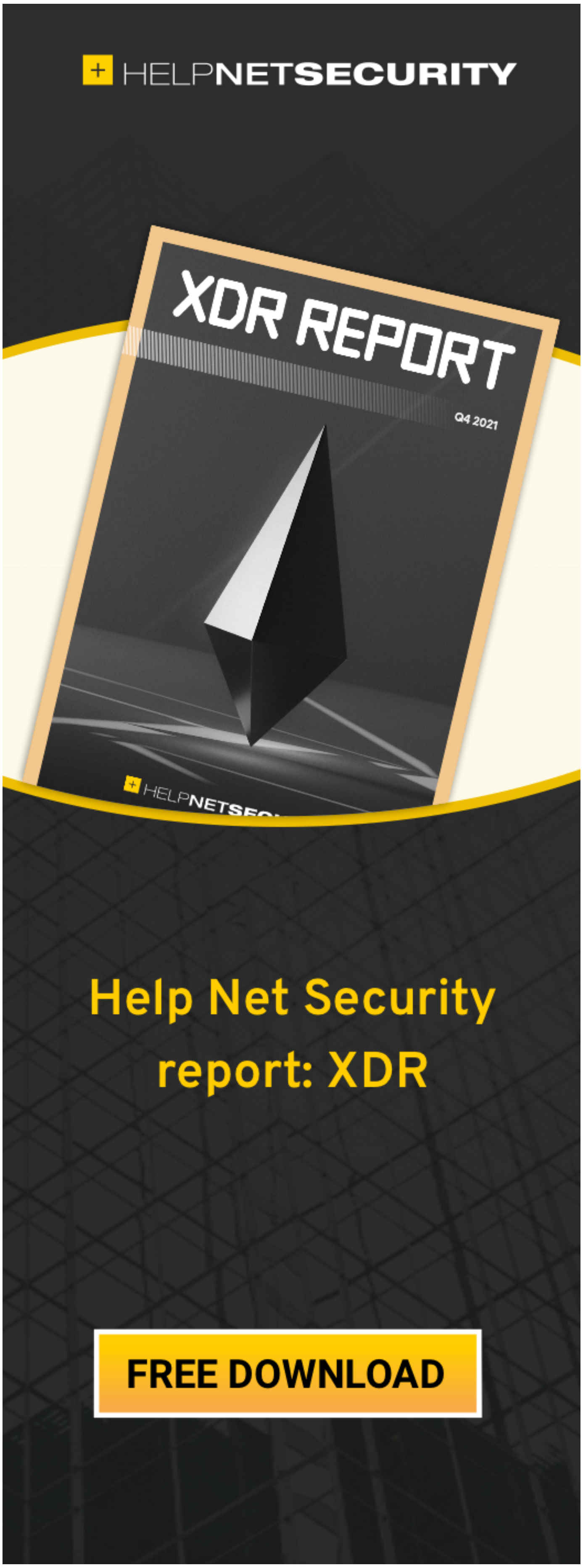
Making micro detection a reality will require a significant paradigm shift.

Making micro detection a reality will require a significant paradigm shift. Application feature functionality and security need to be handled by separate independent teams. Today many companies have developers who are also responsible for security. Separating church and state is important, the fox cannot be in the henhouse, pick your analogy; otherwise, you end up with supply chain issues. What's needed is an agile approach to security and development that brings the two disciplines together to work in conjunction.

The shift may take years, but the current cybersecurity climate has spurred an awakening that is forcing application providers to accept they can't continue to develop software in the same way.

The role for managed detection and response

Managed detection and response will still play a critical role in this new paradigm. MDR's strength is putting organizations in a good security posture to begin with and prioritizing their focus on what needs to be done to prevent a breach. In the event, the organization does get breached, MDR providers can help control the extent of the attack to minimize the impact. The shift toward a security-first development mindset coupled with monitoring by a strong MDR partner will provide the most robust protection in a growing and increasingly aggressive threat landscape.



Supply chain shortages create a cybersecurity nightmare

Guy Gilam

Head of Product Marketing, Cybellum

The White House has recently issued alerts noting that many manufacturers suffer from disrupted supply chains, and rebuilding supply chains is a major priority. Some analysts are suggesting that many months, and perhaps years are likely to transpire before the chaos subsides.

Medical devices manufacturers are not excluded from this disruption. But pausing production until the supply chain is back entirely is not an option. Businesses need to keep production flowing, and that requires finding new suppliers. However, new and potentially less vetted suppliers bring with them new risks and the potential of introducing vulnerabilities and threats into the product or device lifecycle.

The weakest link

As recently reported in the financial press, many major healthcare manufacturers including Phillips and GE Healthcare are suffering from supply chain challenges. The delay of supplies has impacted their ability to meet production expectations for quantity and timelines. Failing to meet these expectations has impacted their bottom line, with noticeable fourth-quarter losses for these organizations.

Failure to deliver

In many cases, the supply line is backed up, due to delays in production or shipping. Even if the components are produced, they cannot promptly make their way to the next steps in the production line. This leads to companies having to pre-order far more components than they would typically store at any given time, to create a stockpile, and ensure their production chain is consistent.

This need for stockpiling or over-ordering, are driving many to seek alternative suppliers who can produce steady supplies. With new suppliers comes the added risk of new, untested components and the potential for new vulnerabilities.

> *With new suppliers comes the added risk of new, untested components and the potential for new vulnerabilities.*

This is where the challenges grow exponentially. When trusted and vetted suppliers are rapidly replaced or augmented, the risk significantly increases of cyber threats and vulnerabilities entering into the product or device lifecycle.

Supply chain issues are already one of the weakest links for an organization, even in the best of times. The challenges are not just in how they impact production capabilities, but also in how they affect the security of the final product. For any complex medical device, many layers of suppliers that provide hardware and software exist. The manufacturer who assembles these components into a final product has limited control and visibility of what's in the various components or software, creating a huge risk for the final product and to its users. Changing suppliers only serves to increase their risk posture.

Vetting new suppliers

Sometimes the only way to circumvent a shortage is to find a different supplier to meet the requirements. This is especially important for medical devices where on-time production and delivery can be a question of life or death.

When a new supplier is onboarded, there is still trust to be built. With no previously existing relationship, there is an increased need for caution, especially when vetting the quality of the supplier's products.

It is imperative at this point to monitor for software vulnerabilities, which is vital for product security. This is the first step because in order to meet the strict FDA requirements for medical devices, it is critical to ensure that the components interoperate, are fault-tolerant, and do not come with any inherent vulnerabilities.

> *When a new supplier is onboarded, there is still trust to be built. With no previously existing relationship, there is an increased need for caution, especially when vetting the quality of the supplier's products.*

Vulnerabilities in code

Anytime code is developed or integrated from an open-source library, there is a possibility of an undiscovered flaw. Any device containing software can have errors in it or in the software libraries it utilizes. Assessing this early in the development process is essential for secure product development and for uncovering vulnerabilities as early as possible, to mitigate risk and minimize damage.

Today, software is more assembled than written, leveraging commercial and open-source software to create the core of the device functionality. These components, while expediting build time, also introduce potential vulnerabilities. For example, until recently the Log4j libraries were considered industry standards and safe open-source additions for logging functionality. In December 2021, these libraries were identified as having a remote code execution (RCE) vulnerability that received the maximum possible CVSS score of 10.0. On discovery, organizations worldwide scrambled to patch and contain this vulnerability before attackers could take advantage of it.

Commercial software is also not exempt from similar high-impact vulnerabilities. The Ripple20 library was also considered a relatively safe and industry-standard software component. Discovery of its vulnerable status left numerous devices open to attack.

> *Commercial software is also not exempt from similar high-impact vulnerabilities.*

The challenges with software components are part of what led to President Biden's Executive Order to help improve software supply chain security through transparency. This order states that Software Bill of Materials (SBOMs) should be available to manufacturers, vendors, and consumers. The SBOM should contain criteria based on the National Telecommunications and Information Administration (NTIA) minimum elements, which include in-depth information about the software components, their versions and dependencies. With this information, organizations can track existing vulnerabilities and new vulnerabilities as they emerge.

Trust but verify

One of the first steps to be taken with a new supplier is to validate their technology from a security point of view. Tracking the results of this effort is critical to identify reliable suppliers and those who may be delivering faulty or vulnerable products. However, verifying the security posture of supplier components and product software is not easy. The source code isn't readily available in many cases, so visibility has to be attained through other routes, such as binary analysis that isn't reliant on having the source code available.

Not every vulnerability assessment tool can deliver accurate results. A reliable solution needs to understand the potential scope and accessibility of vulnerabilities discovered. This information will help to narrow down whether the vulnerability applies to your product.

Using validation and testing tools to assess compiled code, is vital for guaranteeing a product's security that does not provide direct code visibility.

There is too much at stake to trust the supplier when it comes to medical devices. It is crucial to make sure your due diligence is performed with the right solution. Implementing a complete assessment process with the right platform will allow your organization to combat the challenges of new suppliers without sacrificing security.