[+] (IN)SECUREMagazine

09 | 2019
ISSUE 63

CISO challenges

Inside the NIST team working to make cybersecurity more user-friendly

Six criteria for choosing the right security orchestration vendor

Report: Black Hat USA 2019

A NEW PRESCRIPTION FOR SECURITY AND IT'S FREE.

Introducing Qualys Global IT Asset Inventory®

☠ WARNING! SIDE EFFECTS MAY INCLUDE

Actually knowing what's on your global hybrid-IT environment (on prem, endpoints, clouds & mobile)

Improving your security and compliance posture

Better decision making using enriched asset data

Easily finding what you need via automated classification

Finally having clean, uniform data for a single source of truth

Getting that promotion you always wanted

QUALYS.COM /INVENTORY

Qualys®

Table of contents

Featured experts

RANDY BARR, CISO, Topia
CATHERINE CHAMBERS, Senior Product Manager, Irdeto
JIM DUCHARME, VP of Identity Products, RSA Security
JULIE HANEY, co-lead, NIST Usable Cybersecurity team
VLATKO KOSTURJAK, Security Researcher
MATT LOCK, Technical Director, Varonis
NIMMY REICHENBERG, Chief Strategy Officer, Siemplify
MARK SANGSTER, VP & Industry Security Strategist, eSentire
CHARLIE SANDER, CEO, ManagedMethods
MOTTI SORANI, CTO, CyberMDX
MARY THEOFANOS, co-lead, NIST Usable Cybersecurity team

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

Mirko Zorz
Editor in Chief
mzorz@helpnetsecurity.com

Zeljka Zorz
Managing Editor
zzorz@helpnetsecurity.com

Berislav Kucan
Director of Operations
bkucan@helpnetsecurity.com

There is no greater security risk to an organization than a threat actor that knows how to operate under the radar.

Malicious insiders and external cyber attackers are getting savvier and better at blending in without tripping any alerts. They avoid using tools and techniques that trigger standard security systems. How can a company tell them apart from the noise created by legitimate logins to the network that day?

Identifying evasive threats hiding inside the network

AUTHOR_ Matt Lock, Technical Director, Varonis

> *Even the most skilled and meticulous intruders cannot entirely mask their presence within a network.*

The answer lies in context. It is not enough to monitor and log activity throughout the network – organizations need to be able to combine multiple

sources of data to spot the subtle signs of a stealthy attacker at work.

Evasive manoeuvres

Context is important because advanced attackers can use a variety of tactics and tools to stymie established security measures.

For example, they will commonly route their communications through HTTPS and DNS. An average user produces up to 20,000 DNS queries per day: a mind-boggling amount of data that has to be analyzed to detect suspicious traffic, which is especially difficult if the communications present no overtly malicious content. Without any context to enrich this data, analysts will spend too long going through logs to determine if an alert is a genuine threat or a false alarm.

Additionally, activity such as logging into a valid device during business hours and extracting only a small amount of data at a time is unlikely to get flagged as suspicious. Creating shadow accounts with more privileges and granting and removing permissions as needed also helps attackers keep a low profile.

How can advanced threat actors be caught?

Even the most skilled and meticulous intruders cannot entirely mask their presence within a network. The most important factor in detecting them is developing a thorough understanding of the organization's people, processes and technology.

Key actions for detecting hidden threat actors include:

Identifying sensitive data and file access: The first step is to define where your sensitive data is, prioritizing Personally Identifiable Information (PII) and other data governed by regulatory requirements. Then you have to define its "owners" and the accounts that can access it. Any data no longer actively used should be archived to reduce threat vectors.

Managing user permissions: There should be a clear view of all the accounts on the system - normal users as well as service and privileged accounts - and the permissions and access capabilities they possess. Monitoring permission changes can provide a goldmine of valuable information for spotting suspicious behaviour. A least-privilege approach should be used to ensure all users can only access files essential for their job role. Information access should be determined on a need-to-know basis.

> *The signs of an evasive intruder will often be too subtle if data sets are viewed in isolation, and many patterns of suspicious behaviour are only apparent with a unified view.*

Monitoring key systems: It is essential to have visibility of the many systems that can be exploited by attackers. With Windows Active Directory, for example, the company should know information such as account types and server types, privileges, groups, peers, and the difference between personal devices and public workstations.

Initiating high-value user profiling: Correlating user activity to specific devices will help detect subtle signs of an intruder logging into different machines but not doing anything overtly malicious. Understanding the difference between how public and personal devices are used will also help reduce noise and false positives.

Correlation is key

The most important step is to correlate all this data. The signs of an evasive intruder will often be too

Armed with a thorough understanding of what normal behaviour looks like and a unified view of all activity on the network, organizations will be able to make high value correlations that identify some of the most elusive signs of malicious activity.

subtle if data sets are viewed in isolation, and many patterns of suspicious behaviour are only apparent with a unified view. Considering the vast amounts of data flowing through an organization on any given day, this can only be achieved with an automated approach powered by machine learning.

Armed with a thorough understanding of what normal behaviour looks like and a unified view of all activity on the network, organizations will be able to make high value correlations that identify some of the most elusive signs of malicious activity. For example, a user accessing a VPN and then logging into another employee's device will not trigger a standard security system, but such behaviour would be very unusual for a legitimate user and is a clear sign someone has had their credentials phished.

With sufficient data, organizations can go beyond individual users and build peer relationships into their behavioural analytics. This will allow them to quickly spot a user that is displaying unusual file activity compared to their peers, significantly reducing incident response times. Once organizations can reliably detect these signs, even the most evasive attackers will have few places left to hide inside the network.

Inside the NIST team working to make cybersecurity more user-friendly

AUTHOR_ Zeljka Zorz, Managing Editor, (IN)SECURE Magazine

Cybersecurity is usually not a user's primary duty, yet they suffer an increasing burden to respond to security warnings, maintain many complex passwords, and make security decisions for which they are not equipped.

This is the main reason why security needs to be usable and why the National Institute of Standards and Technology (NIST) has a team of researchers working on projects aimed at understanding and improving the usability of cybersecurity software, hardware, systems, and processes.

"Our team works towards influencing cybersecurity standards and guidelines. For example, we were responsible for the inclusion of usability considerations in the NIST Special Publication 800-63 Digital Identity Guidelines," says Mary Theofanos, the leader of the NIST Usable Cybersecurity team.

“We have also increased efforts to actively share NIST’s usable cybersecurity research with security practitioners, managers, end users, and other researchers who can apply our findings and offer feedback on the value and direction of our projects. For example, our phishing research has been a popular topic that we’ve presented at academic research conferences, security practitioner forums, and organization-wide security days.”

> *Users still have a nebulous idea of the consequences of bad security.*

With an academic background in mathematics and computer science and many years of work at the Oak Ridge National Laboratory and US federal agencies under her belt, Theofanos moved to NIST around 2003 to develop standards for usability. She is a convenor of an ISO Working Group developing user-centered design standards and has worked to apply user-centered design and usability principals to many domains including cloud computing, public safety communications and biometrics.

Julie Haney, the other co-lead for the Usable Cybersecurity program, ended up at NIST after getting degrees in CS, spending over 20 years working at the US Department of Defense as a cybersecurity professional and technical leader primarily in the cyber defense mission, and getting increasingly interested in the intersection of people and security and the factors impacting people’s willingness and ability to adopt security best practices and technologies.

“Several years ago, I returned to school to more formally study this area through the Human-centered Computing program at University of Maryland, Baltimore County, where I obtained a master’s degree and am now close to completing my PhD. I began working at NIST so that I could focus specifically on research in the usable cybersecurity area while being afforded the opportunity for my research to have a real-world impact on NIST’s standards, guidelines, and community partners,” she shared.

Such a specific vantage point gives them a singular view and insight on things that all participants in the wider cybersecurity sphere could do to raise the security bar.

Here’s an example: even though people are increasingly exposed to cybersecurity and privacy in the news and they profess to be concerned about their online privacy, they often take no action to protect it.

This is partly because most people don’t know how to protect themselves, partly because usable interfaces for changing security and privacy settings and informing users of privacy issues are not readily available, and partly because they suffer from “security fatigue.”

> *The threat/risk of immediate financial repercussions is just about the only thing that gets users interested in security.*

“We found that the security fatigue users experience contributes to their cost-benefit analyses in how to incorporate security practices and reinforces their ideas of lack of benefit for following security advice,” Theofanos noted. “With respect to security, people expressed a sense of resignation, loss of control, fatalism, risk minimization, and decision avoidance.”

In certain circumstances, many users are ready to take mental shortcuts that will allow them not to give a second thought to security. For example, in a workplace setting, many tend to rely too much on

the organizational safeguards (e.g., email servers, firewalls) to protect them.

Making users care and be careful is not easy

Too many users are still choosing convenience over security. Security measures mean unwelcome friction when you just want to quickly set up an account to buy or do something online, and users still have a nebulous idea of the consequences of bad security.

Even if personal information is disclosed in a data breach, individuals might not experience any immediate, tangible harm, Haney explained. For the same reason, they care little about companies looking at their web activity or the security of consumer Internet of Things.

> *People need to first understand how security is applicable to them and then be provided simple, actionable guidance.*

"We're currently conducting a study to understand people's experiences with and perceptions of smart home technologies. What we're finding is that most people are not concerned about the privacy of the information being collected by their smart home devices. They feel that, because they're not doing anything illegal, they have nothing to hide. They are also numb to their private information already being out there on the internet. Or, if they are concerned, they're willing to accept the risks for the convenience of the devices," Haney shared.

"Even fewer are concerned about smart home security. To them, the security threat consists of a nebulous group of hackers who likely would not be interested in targeting them directly. Therefore, they are not motivated to take action or learn about what they can do to protect themselves."

In fact, the threat/risk of immediate financial repercussions is just about the only thing that gets users interested in security.

> *To motivate their audiences to engage in beneficial security behaviors, cybersecurity advocates first have to establish trust with their audience.*

The financial sector is aware of that and is definitely investing in usable security to take the burden off users while increasing the underlying security of their systems and online services. However, Haney noted, many smaller businesses remain oblivious to the risks to their businesses and customers and/or lack the resources and skill to do anything about it.

Advice for security advocates

While there's a dire need for those who design security technologies, interfaces, and processes to consider user needs and context and make it easy for them to do the right thing, security advocates are also needed to promote, educate about, and encourage security adoption.

As Haney and a colleague discovered after polling cybersecurity advocates from industry, higher education, government, and non-profits, non-technical audiences find security to be scary, confusing and dull.

To motivate their audiences to engage in beneficial security behaviors, cybersecurity advocates first have to establish trust with their audience. They should do so by demonstrating technical knowledge and by flexing their interpersonal skills to build relationships.

Next comes the task of overcoming those three negative perceptions of security.

To make security less confusing and complex, security advocates should avoid technical jargon and reframe highly technical concepts using terms their audience can understand.

"Advocates must strike a careful balance between being candid about security risks while being hopeful and encouraging. The latter are essential for developing a sense of empowerment in the audience. Too much fear can be debilitating," Haney noted.

To make security less confusing and complex, security advocates should avoid technical jargon and reframe highly technical concepts using terms their audience can understand. The security message must be tailored to the audience's context – their environment, constraints, concerns, and skill level – and include simple, practical recommendations commensurate with it.

Finally, advocates must overcome perceptions that security is irrelevant and boring by exhibiting enthusiasm, making security relatable, and incentivizing security behaviors (i.e., motivating people to take action). "They should not hesitate to think out-of-the-box and try novel awareness and education approaches," she concluded.

Organizational cybersecurity problems

Organizations have their own specific cybersecurity blind spots, Theofanos and Haney said.

Some don't fully understand or relate to the security risk so they don't prioritize security, while others choose the opposite end of the spectrum: they push towards the most secure and restrictive solutions without regard for the impact on users, resulting in user frustration (best-case scenario) or users circumventing the security to cope with the additional burden (worst-case scenario).

"We also have observed a compliance mentality among many organizations, where compliance to a security directive or guideline is seen as success without regard for effectiveness," they added.

"This is especially problematic for security awareness training. Many organizations have an annual security awareness training mandate for which success is measured by the number of people in the workforce who have taken the training. However, this number tells us nothing about how effective the training is in teaching and changing behavior."

Security awareness trainings should also be revamped, they feel.

"The current model of 'death by PowerPoint' or computer-based annual security training is not working. Scare tactics without actionable guidance are also not working. People need to first understand how security is applicable to them and then be provided simple, actionable guidance," they pointed out.

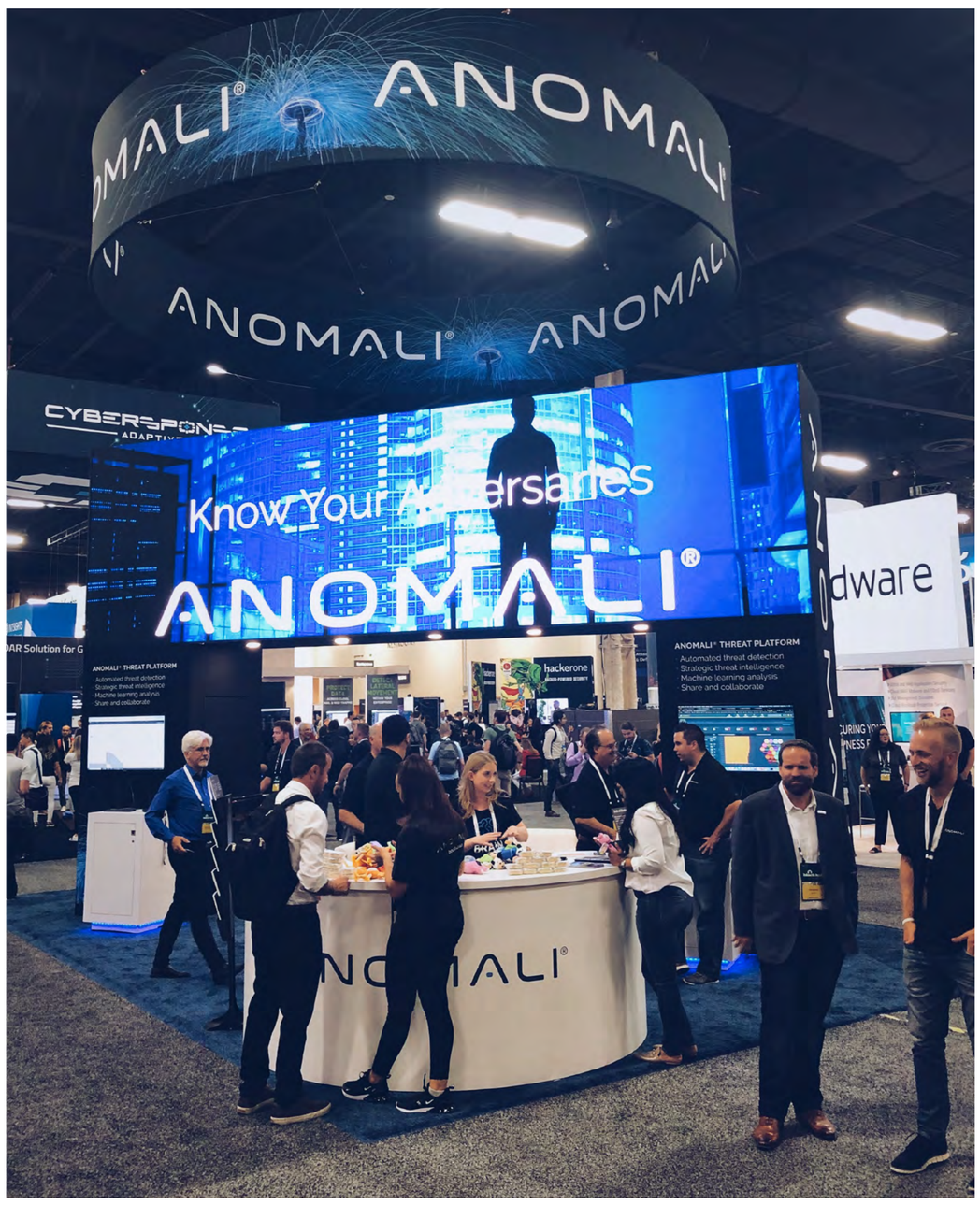
Conversely, a thing Theofanos and Haney would like to see less of is the "us vs. them" mentality between security professionals and users: security professionals should be more aware of the human element and find a way to work with users as partners in facing cybersecurity problems, not as enemies or burdens.

REPORT:

Black Hat USA 2019

Black Hat USA 2019 welcomed more than 20,200 of the most security-savvy professionals across the InfoSec spectrum – spanning academia, researchers, and leaders in the public and private sectors. The event's robust lineup featured groundbreaking content led by security experts who showcased the latest and greatest research currently impacting the industry.

The Black Hat Review Board, comprised of 24 security experts, evaluated more submissions this year than ever before – producing the largest program to date. This year's conference welcomed more than 500 speakers and Trainers across more

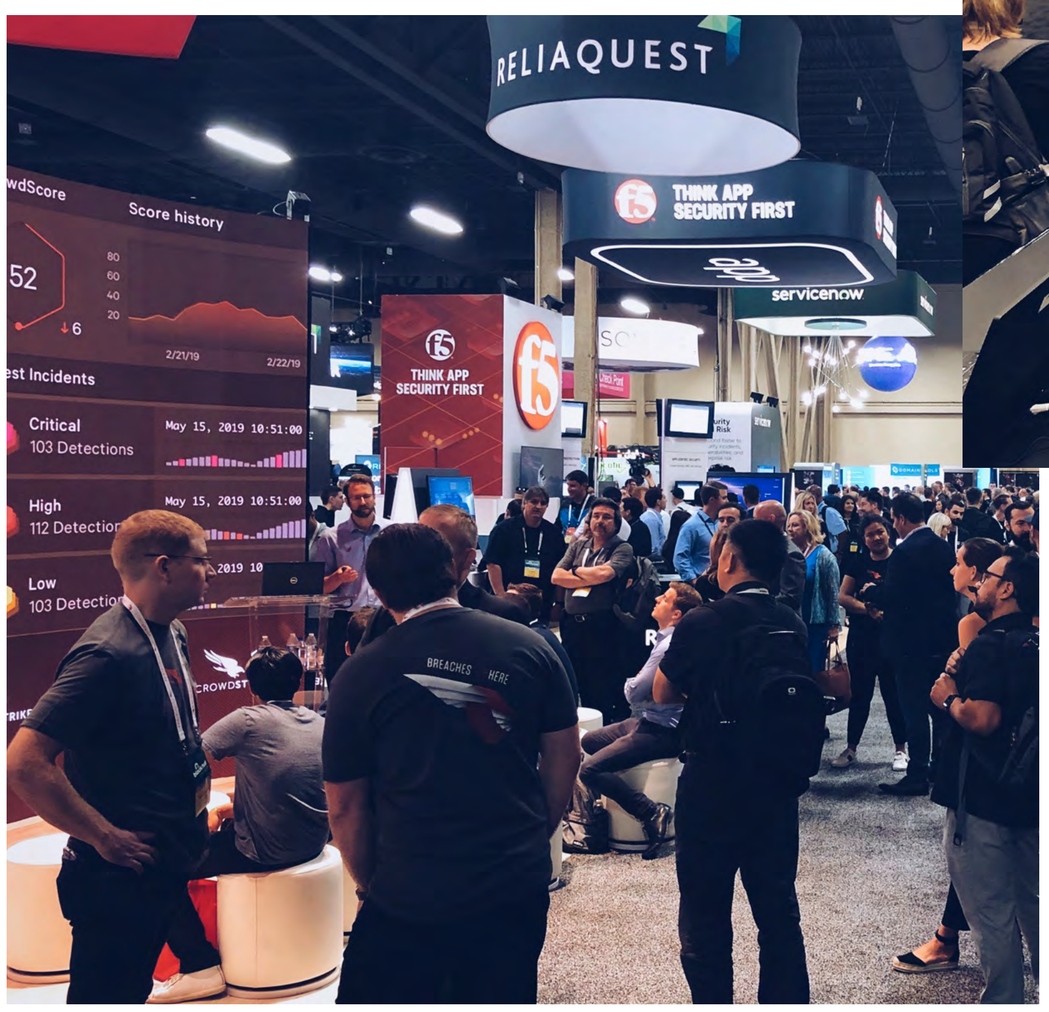


than 90 deeply technical Trainings and more than 120 innovative research-based Briefings on stage.

Show highlights

- **Keynote Dino Dai Zovi,** responsible for leading security engineering for Square's Cash App, presented "Every Security Team is a Software Team Now" to a bustling Mandalay Bay Events Center, which housed more than 5,500 attendees.
- **CISO Summit** welcomed 200 executives from top public and private organizations for an exclusive, program intended to give CISOs and other InfoSec executives more practical insight into the latest security trends and technologies and enterprise best practices.
- **Arsenal** returned for its tenth year, offering researchers and the open source community the ability to demonstrate tools they develop and use in their daily professions – live. This year's program showcased more than 90 tools and featured the all-new Arsenal Lab, which offers a hands-on opportunity to play with hardware, ICS gear, and IoT devices.
- **Business Hall** buzzed with more than 300 leading companies. Attendees were given the opportunity to experience hands on learning, demonstrations and education on the latest products and technologies impacting the industry, as well as deep dive sessions presented by vendors in the Business Hall Theaters.
- **Electronic Frontier Foundation Support**: For the sixth year, Black Hat is proudly donating $50,000 to the EFF to continue supporting their important work in protecting civil liberties within the digital world. Black Hat has a strong partnership with the EFF to provide pro-bono legal consultations to security researchers on the legality of any research or data they plan to present at the annual shows.
- **Scholarships**: Black Hat awarded more than 300 Academic Briefings Scholarships to deserving students from around the world. Black Hat and EWF again offered the Female Leaders Scholarship Program to minimize the gender gap among the InfoSec community and give students the opportunity to learn, network and collaborate with the world's brightest minds. Event speakers were also given two complimentary Briefings passes per talk to be given to students of their choice.
- **QueerCon**: Black Hat will be donating all proceeds from its specialized 2019 event t-shirt to QueerCon, the largest social network of LGBT hackers from around the world.

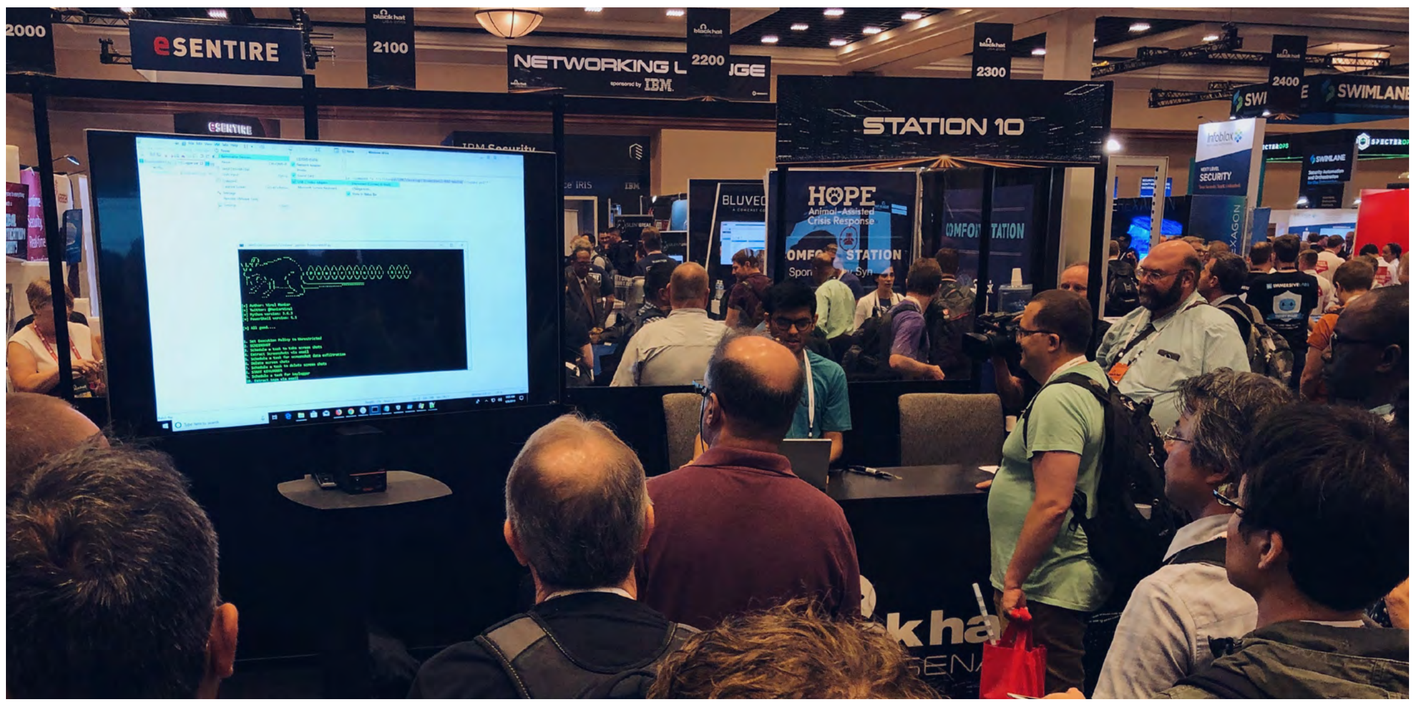
BLACK HAT USA 2019 gallery



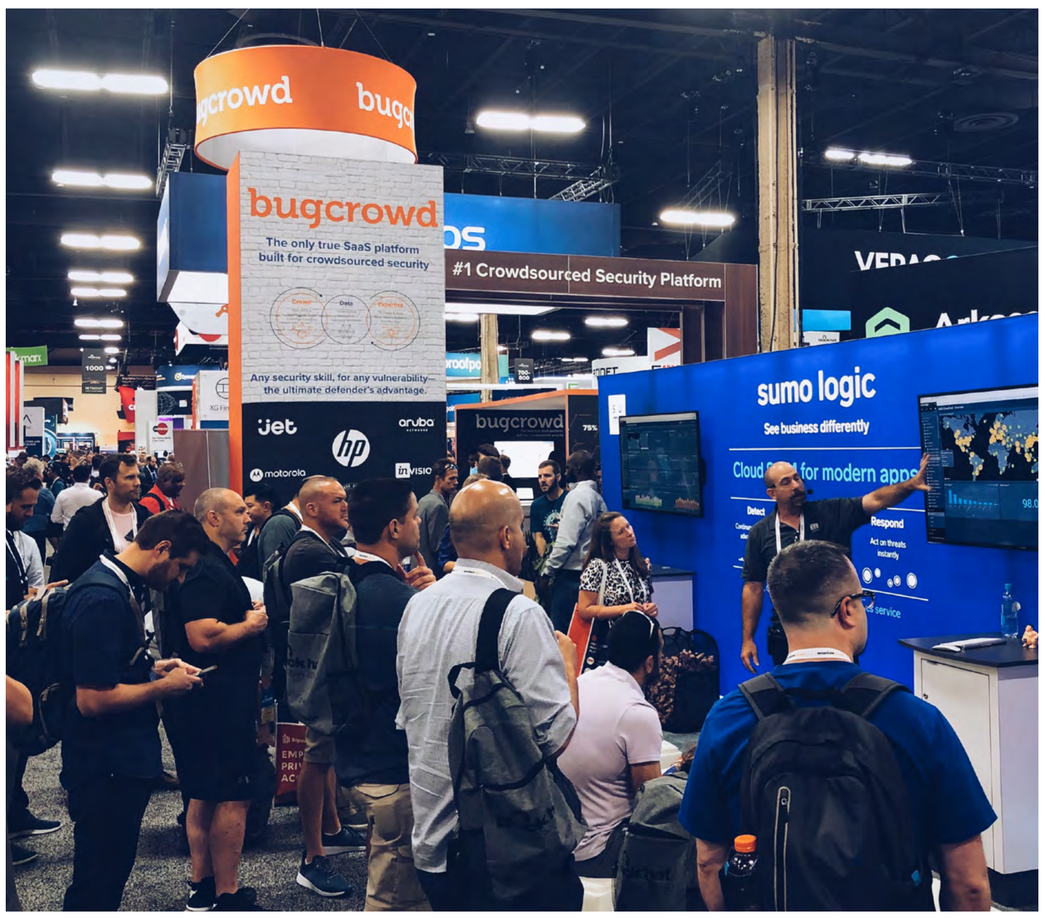

Qualys. Enterprise
Asset Inventory
Global IT Assets
DASHBOARD
INVENTORY
OPERATING SYSTEM DISTRIBUTION
TOP CLIENT OPERATING SYSTEM
TOP SERVER OPERATING SYSTEM
TOP CLIENT HARDWARE
TOP SERVER HARDWARE
QUALYS.COM /INVENTORY


ir.deta
Blend to defend
cloakware by ir.deta

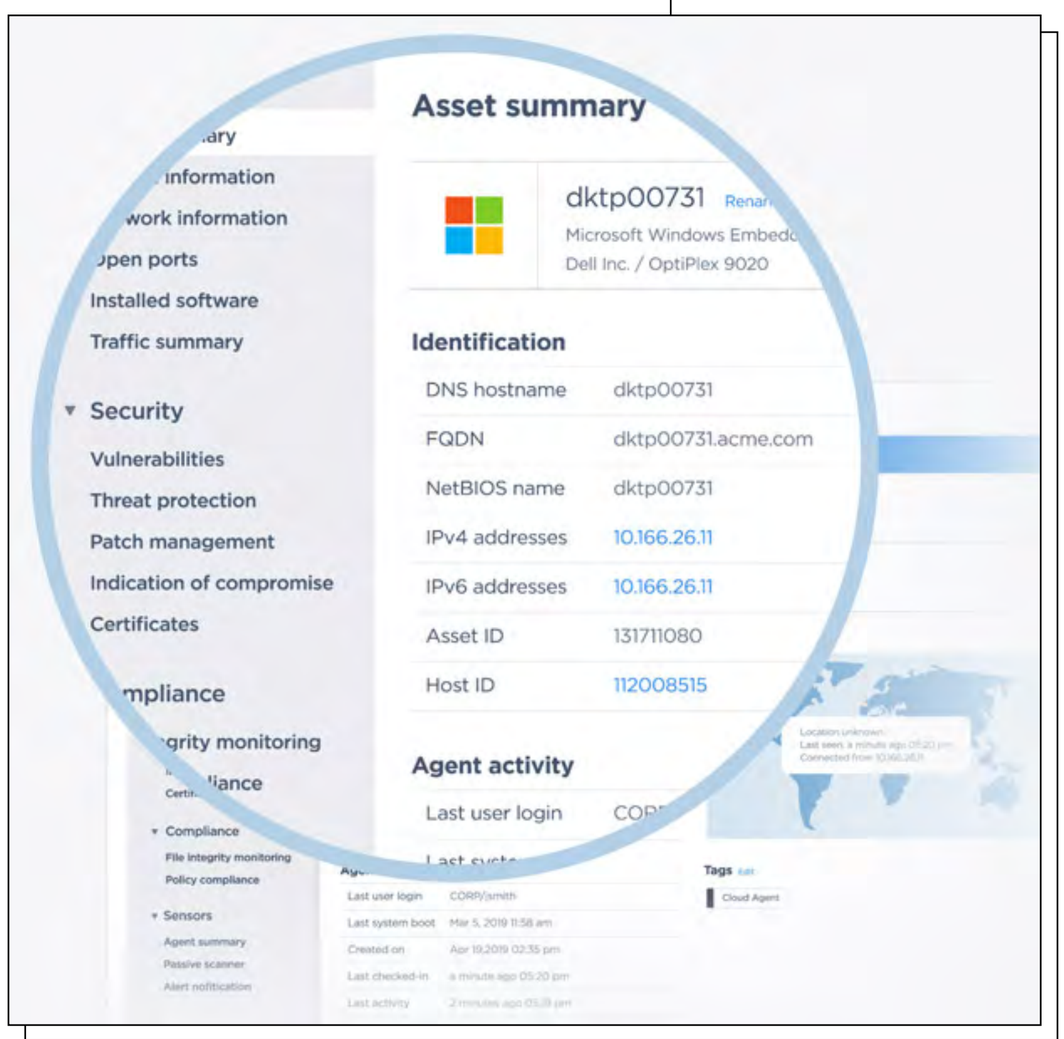

SOUTH CONVENTION CENTER
MANDALAY BAY BALLROOM • SOUTH SEAS BALLROOM
BAYSIDE • SHORELINE • OCEANSIDE • PALM
black hat USA 2019

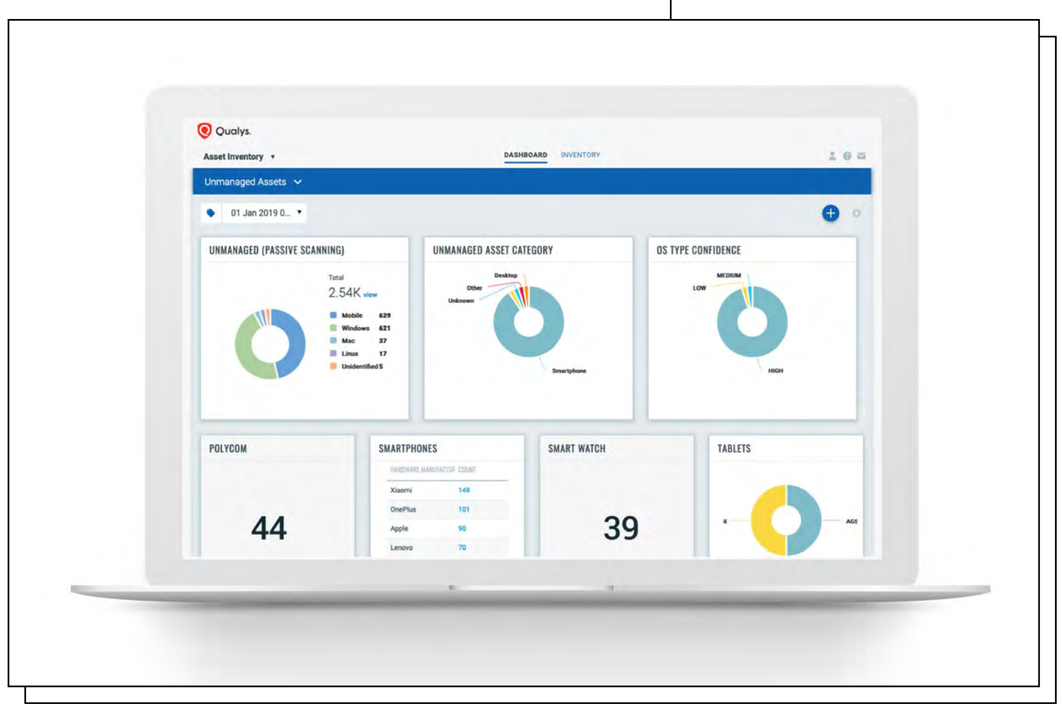

eSENTIRE
NETWORKING
STATION 10
HOPE
SECURITY

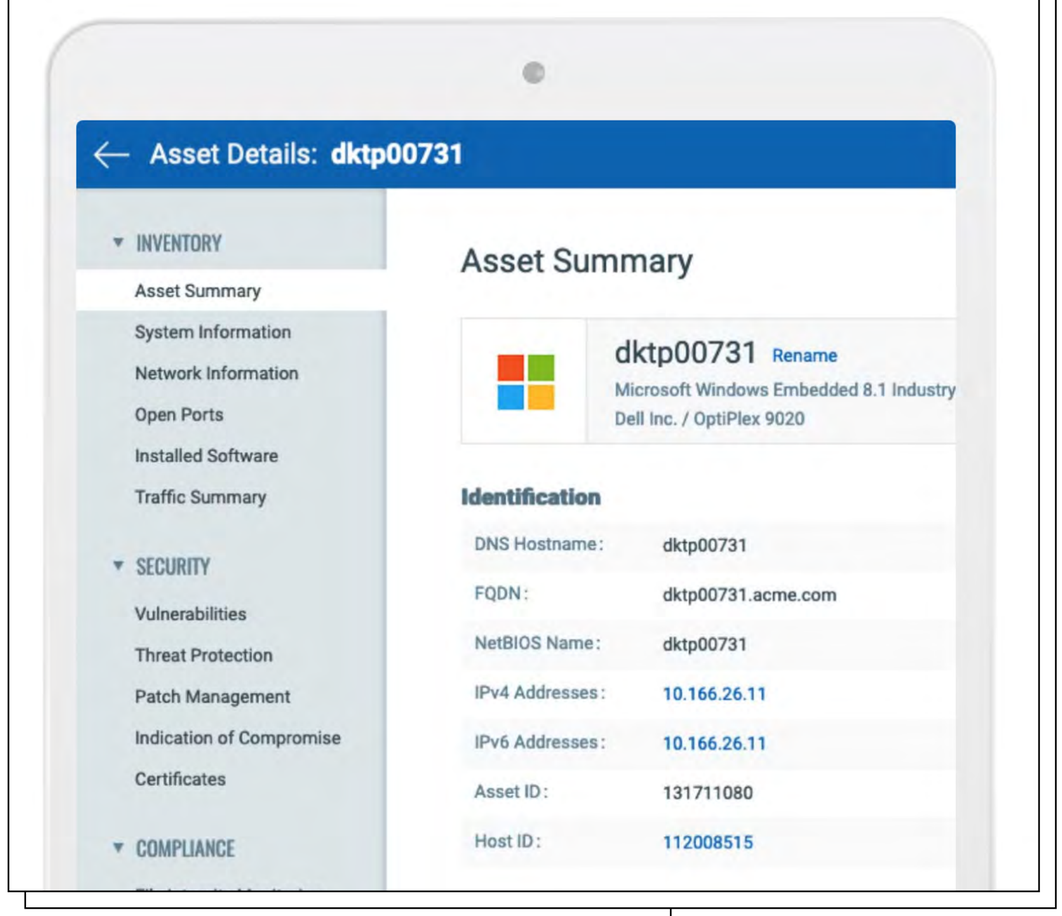

eSENTIRE
See everything. Miss nothing.
Human expertise at machine scale
DEVO
Alert Fatigue & Attrition
Demo & Dice


bugcrowd
The only true SaaS platform built for crowdsourced security
#1 Crowdsourced Security Platform
sumo logic
See business differently

Qualys is making its Global IT Asset Discovery and Inventory app available to all businesses for free







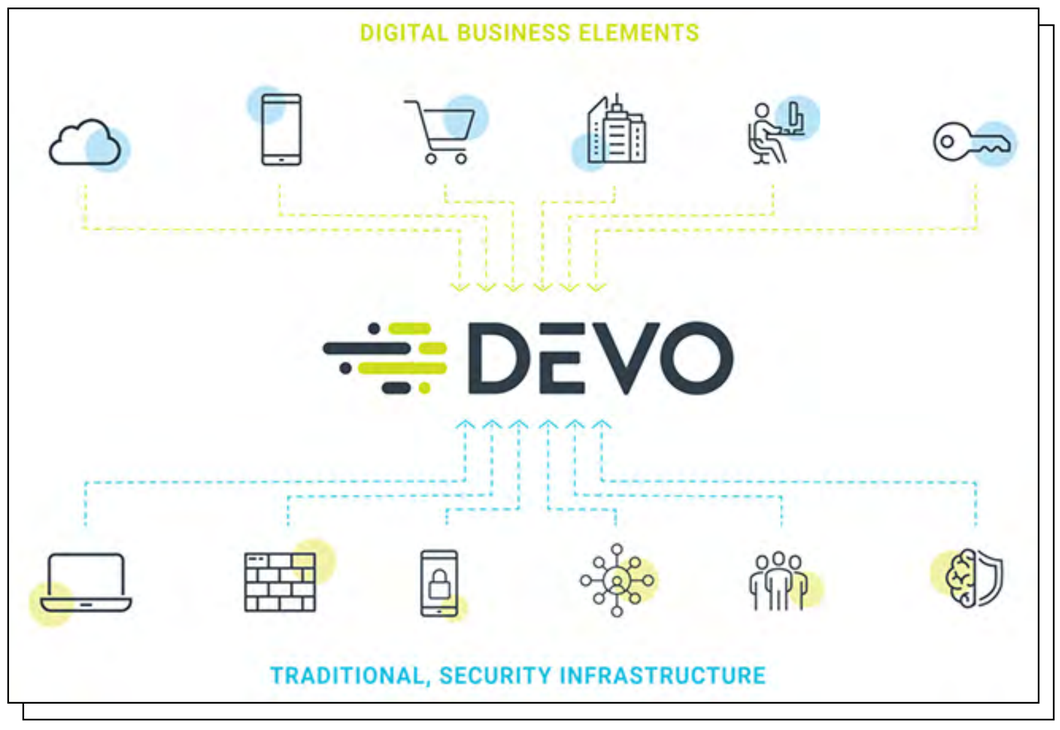
Qualys is making its Global IT Asset Discovery and Inventory app available to all businesses for free. In a world where connected devices are exploding, visibility across all devices and environments is critical.

With the free Global IT Asset Discovery and Inventory app (qualys.com/inventory), you can:

- Automatically create a continuous, real-time inventory of known and unknown assets across your global IT footprint. The assets can be any assets from on-premises, endpoints, multi-cloud, mobile, containers, OT and IoT.
- Automatically classify, normalize, and categorize assets to ensure clean, reliable, and consistent data. In-depth asset details provide fine-grained visibility on the system, services, installed software, network, and users.
- Search across millions of assets and have full visibility of any device in seconds.
- Instantly detect any device that connects to your networks, via our passive scanning technology. Upon an unknown device detection, users can install a light-weight Qualys self-updating agent (3MB) to turn the device into a managed device or launch a vulnerability scan.

Devo Technology defines vision for next-gen cloud SIEM

Devo Technology, the data analytics company that unlocks the full value of machine data for the world's most instrumented enterprises, previewed its next-gen cloud SIEM at Black Hat USA 2019.



Digital transformation is creating rapidly growing volumes of data, leading to new vulnerabilities and attack vectors, while adversaries are growing increasingly more sophisticated. As a result, SOCs are struggling to fulfill their critical mission of identifying and eliminating threats. With the industry's current solutions, analysts lack visibility across the expanding attack surface, are overwhelmed by the volume of security alerts, and struggle to reliably identify and act on threats due to a lack of context about the threats and entities involved.

"The effectiveness of the SOC, and cybersecurity as a whole, comes down to the effectiveness of security analysts. It is quite obvious that legacy SIEMs fail to provide the visibility, insight, and workflows required to support the modern analyst," said Julian Waits, General Manager of Cyber, Devo. "Devo empowers SOC analysts by harnessing their intuition, creativity, and expertise, arming them with the latest technology vital to furthering their mission to stop material threats."

Devo believes all data has the potential to inform and improve cybersecurity. The next-gen SIEM must evolve to become the central hub for all data and processes within the SOC, not simply provide alert management for traditional security events. This will empower analysts to visualize the threats that matter most to the business, improve the speed and accuracy of triage, investigation, and response, and magnify the intuition of analysts.

SentinelOne enhances container and cloud-native workload protection

SentinelOne, the autonomous endpoint protection company, announced the availability of the next generation of its server and workload protection offering.

The new product, purpose-built for containers, including managed or unmanaged Kubernetes systems, delivers SentinelOne's patented Behavioral AI and autonomous response capabilities across all major Linux platforms, physical and virtual, cloud-native workloads, and containers, providing prevention, detection, response, and hunting for today and tomorrow's cyber threats. This includes malicious files and live attacks across cloud-native and containerized environments, offering advanced response options and autonomous remediation.

Capsule8 Protect now solves production security's data warehousing problem

Capsule8 announced Investigations, new functionality that adds full endpoint detection and response (EDR)-like investigations capabilities for cloud workloads to Capsule8 Protect, its high-performance attack protection platform for Linux production environments.

An industry-first cloud investigation capability, Capsule8's Investigations is designed to remove the manual effort required to maintain a dedicated database just for security data – enabling customers to quickly determine what transpired in an incident (who, what, when, where).

By leveraging cloud native technologies, including AWS Athena and Google's BigQuery, organizations can create an on-demand database and make that data accessible for security practitioners seeking additional context about alerts and system activities. This also creates a feedback loop for security teams to investigate an incident, figure out why it happened, and refine automated response actions to prevent it in the future. Importantly, Investigations reimagines security as a data warehousing problem and enables cloud users to receive the benefit of a scalable data pipeline with minimal setup and maintenance.

Capsule8 Protect is the industry's only high-performance, real-time attack protection platform purpose-built for Linux production environments – whether containerized, virtualized or bare metal. The platform monitors a customer's entire Linux infrastructure, detecting and preventing attacks and other unwanted activity to keep the production environment safe and stable – in the cloud, containers or on-prem alike. Capsule8 helps companies of any size collect and understand all the data needed to protect themselves, without having to reinvent the wheel with costly manual effort.

Signal Sciences launches new application security solution for Envoy

Signal Sciences the general availability of the industry's first application security solution for Envoy via its award-winning next-gen web application firewall (WAF) and runtime application self-protection (RASP) solution.

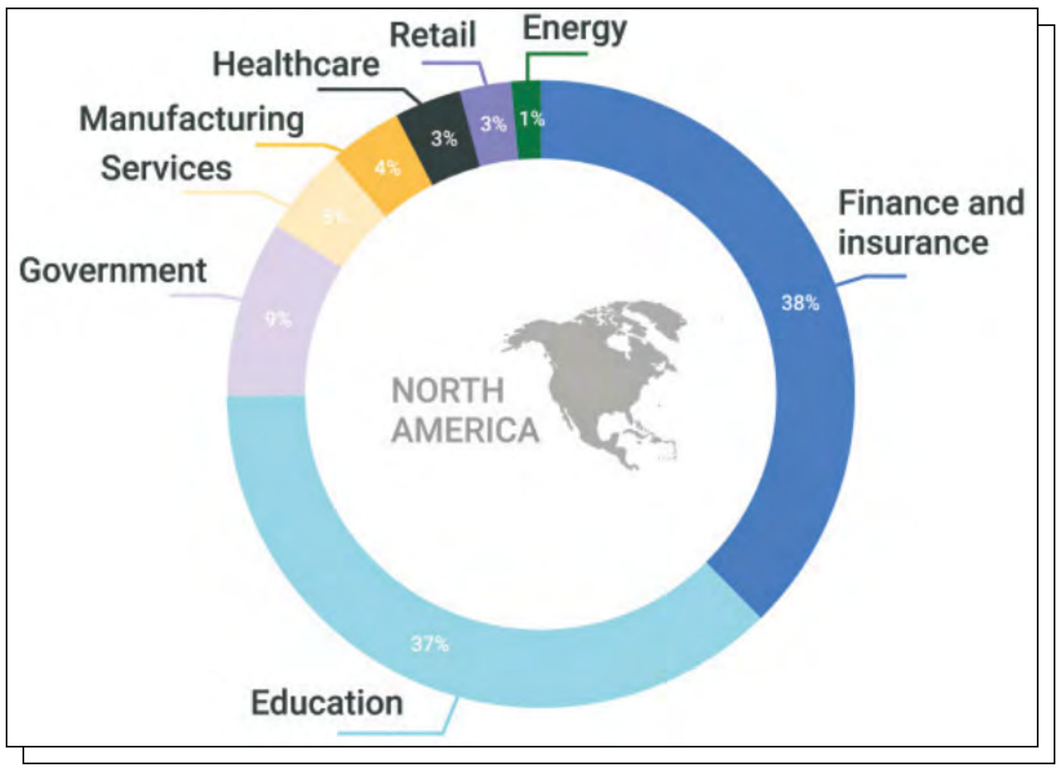
As organizations move to cloud-native applications and services, Signal Sciences makes it effortless to achieve advanced Layer 7 security and comprehensive visibility at scale for one of the most cutting-edge cloud application networking technologies today. This expands Signal Sciences container and microservices protection offering, and gives customers utilizing Envoy even greater flexibility to implement web application and API security for any app or service on any infrastructure.

What's cybercriminals' most effective weapon in a ransomware attack?

Cybercriminals' most effective weapon in a ransomware attack is the network itself, which enables the malicious encryption of shared files on network servers, especially files stored in infrastructure-as-a-service (IaaS) cloud providers, says Vectra.

Attackers today can easily evade network perimeter security and perform internal reconnaissance to locate and encrypt shared network files. By encrypting files that are accessed by many business applications across the network, attackers achieve an economy of scale faster and far more damaging than encrypting files on individual devices.

According to the Vectra 2019 Spotlight Report on Ransomware, recent ransomware attacks cast a wider net to ensnare cloud, data center and enterprise infrastructures. Cybercriminals target organizations that are most likely to pay larger ransoms to regain access to files encrypted by ransomware. The cost of downtime due to operational paralysis, the inability to recover backed-up data, and reputational damage are particularly catastrophic for organizations that store their data in the cloud.



PERCENTAGE OF THE TOTAL NUMBER OF INCIDENTS EXHIBITING RANSOMWARE NETWORK FILE ENCRYPTION PER INDUSTRY IN NORTH AMERICA, FROM JANUARY-JUNE 2019

"The fallout from ransomware attacks against cloud service providers is far more devastating when the business systems of every cloud-hosted customer are encrypted," said Chris Morales, head of security analytics at Vectra. "Today's targeted ransomware attacks are an efficient, premeditated criminal threat with a rapid close and no middleman."

CrowdStrike CrowdScore enables CxOs to see their org's real-time threat level

CrowdStrike launched CrowdScore, a new industry innovation on the CrowdStrike Falcon platform. CrowdScore is a simple metric that enables CxOs to instantly see the real-time threat level their organizations are facing, allowing them to quickly mobilize resources to respond.

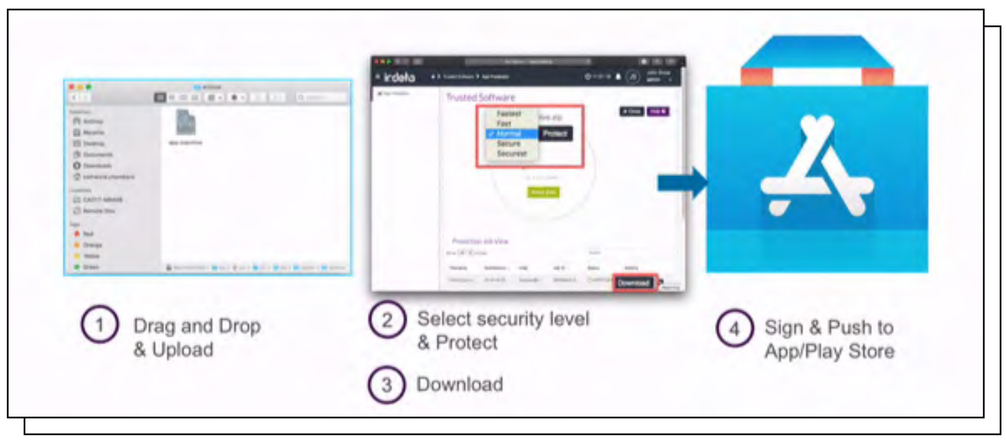
Speed of detection, investigation and response are essential for effective security. CrowdStrike research on breakout time shows that security teams should strive to detect threats on average in 1 minute, understand them in 10 minutes and contain them in 60 minutes to be effective at stopping breaches.

Irdeto Trusted Software: Automated iOS and Android app protection

Irdeto has announced Trusted Software, a new service designed to offer optimal flexibility and efficiency to developers and organizations facing today's cybersecurity challenges. Hosted in the cloud, Trusted Software automates iOS and Android app protection with a simple drag-and-drop interface. Optimized with machine learning, the new service provides organizations with assurance that apps are provided with expert-level protection against hackers and cyberthreats.

Unlike other solutions on the market, which typically require cybersecurity expertise to configure, build and apply proper protection, Trusted Software takes app-store-ready applications as a starting point. Trusted Software then returns a protected application that is ready for posting to the app store, eliminating the need for the organization to spend time or resources securing mobile apps. The new service also prevents organizations from needing to develop or hire the necessary skillsets to ensure proper cybersecurity of mobile apps is obtained.

"We recognize that businesses today have to balance many different priorities when it comes to cybersecurity," said Jaco Du Plooy, Vice President of IoT Security, Irdeto. "We also realize that many organizations do not have the staff, budget or resources to protect every application that they either develop or use. That's where we come in. With Irdeto Trusted Software, we eliminate the need for organizations to secure their own applications, leaving that process to us. Using Machine Learning to identify and target critical code that requires protection, our new solution provides protection that can be applied by the app developer, without any special expertise, in no time at all."



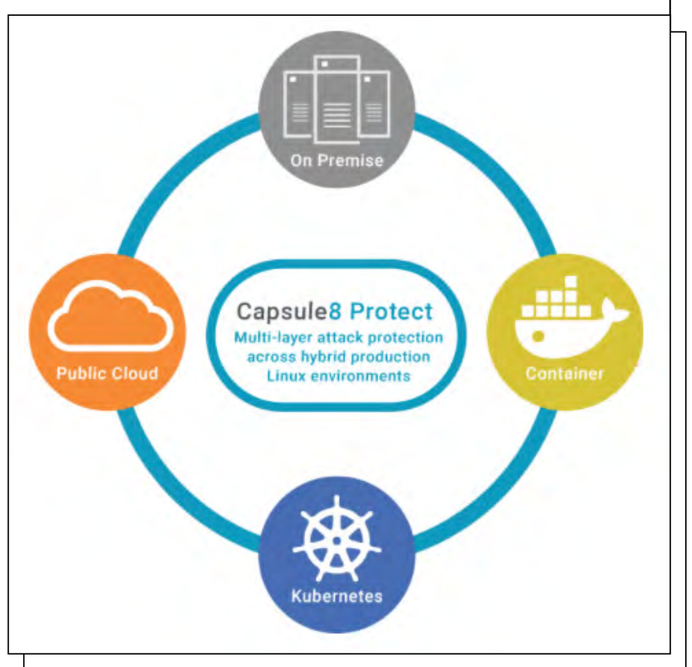
Aporeto launches zero trust cloud security solution for Kubernetes multi-cluster deployments

Aporeto announced its cloud network security solution for seamless distributed policy management across Kubernetes multi-cluster and container environments, using a unique application identity-based approach to security instead of relying on IP addresses. Aporeto's use of identity enables network security policies to now be managed up the stack at the application level.

Code42 Next-Gen Data Loss Protection solution helps companies spot data theft when employees quit

Using Code42 Next-Gen Data Loss Protection, organizations can detect risky file activity across computers and the cloud as well as quickly investigate unusual file behavior and respond to data loss, leak and theft. At any point in time, Code42's solution can tell organizations where their data lives, when and what data leaves, and who has, or ever had, access to it.

Capsule8 announces multimillion-dollar investment from Intel Capital



Capsule8 announced a multimillion-dollar investment from Intel Capital. The rapidly growing company will apply the funds to drive a range of sales, marketing, product development and customer-facing initiatives. Intel joins existing investors ClearSky Security, Bessemer Venture Partners and other strategic investors, bringing the total funds raised by Capsule8 to $30 million.

Capsule8 delivers high-performance attack protection for Linux production environments – whether containerized, virtualized or bare metal, deployed on-premises or in the cloud. Safe for the busiest workloads in the largest clusters, the company's flagship platform, Capsule8 Protect, replaces multiple legacy controls with a single solution that detects and prevents exploits in real-time – while preserving the performance and reliability of production infrastructures.

Scalable and cloud-agnostic, Capsule8 Protect features an "API-first" architecture for seamless technology integration, enabling enterprises to capitalize on existing investments.

Onapsis Platform helps optimize and protect business-critical apps

Onapsis, the leader in business-critical application protection, announced the latest release of the Onapsis Platform, which delivers next-generation actionable insight, change assurance, automated governance and continuous monitoring capabilities to help optimize and protect business-critical applications. The Onapsis Platform is designed for cross-functional collaboration among the IT, cybersecurity, development and GRC teams responsible for business-critical application performance and protection, allowing them to optimize workflows, automate manual tasks and reduce costs.

ID Experts launches new free CyberScan dark web and social media scanning product

ID Experts announced public availability of its new free CyberScan dark web and social media scanning product. Unlike other free dark web offerings, CyberScan not only perpetually scans all levels of the dark web – surface, dark and deep – for the user and provides them with ongoing monitoring and protection, but it reaches a third more of the dark web than other services. It also includes ID Experts' innovative new SocialSentry privacy protection service for Facebook users.

Security news

A point-in-time approach to risk management is no longer effective

Among organizations that engage third parties to provide business services, 83% identified third-party risks after conducting due diligence and before recertification, according to Gartner.

Gartner's survey of more than 250 legal and compliance leaders reveals that the standard point-in-time approach to risk management is no longer effective in today's landscape of fast-paced, rapidly changing business relationships.

With an increasing number of third parties performing new-in-kind and noncore services for organizations, material risks cannot always be identified prior to the start of a business relationship. Modern risk management must account for ongoing changes in third-party relationships and mitigate risks in an iterative way — that is, on a continual basis, rather than at specified intervals.

"Legal and compliance leaders have relied on a point-in-time approach to third-party risk management, which emphasizes exhaustive upfront due diligence and recertification for risk mitigation," said Chris Audet, research director for Gartner's Legal & Compliance practice. "Our research shows an iterative approach to third-party risk management is the new imperative for meeting business demands for speed and stakeholder demands for risk mitigation."

Growing cloud adoption introduces visibility gaps and security complications

As the quantity and frequency of advanced threats continue to accelerate, a new SANS Institute survey found that a continued lack of visibility and the complexity of managing data across on-premises and cloud infrastructures further complicates the battle against such threats.

When it comes to major gaps in the security analytics of their cloud-based infrastructure:

- More than half of the respondents expressed concerns about integrating data with analytics tools and combining data across cloud environments.
- Nearly 55 percent struggle with a lack of integration between current security analytics tools and cloud infrastructure.
- Approximately 43 percent faced a lack of threat insights targeting cloud environments.

The changing face of DDoS attacks: Degraded performance instead of total takedown

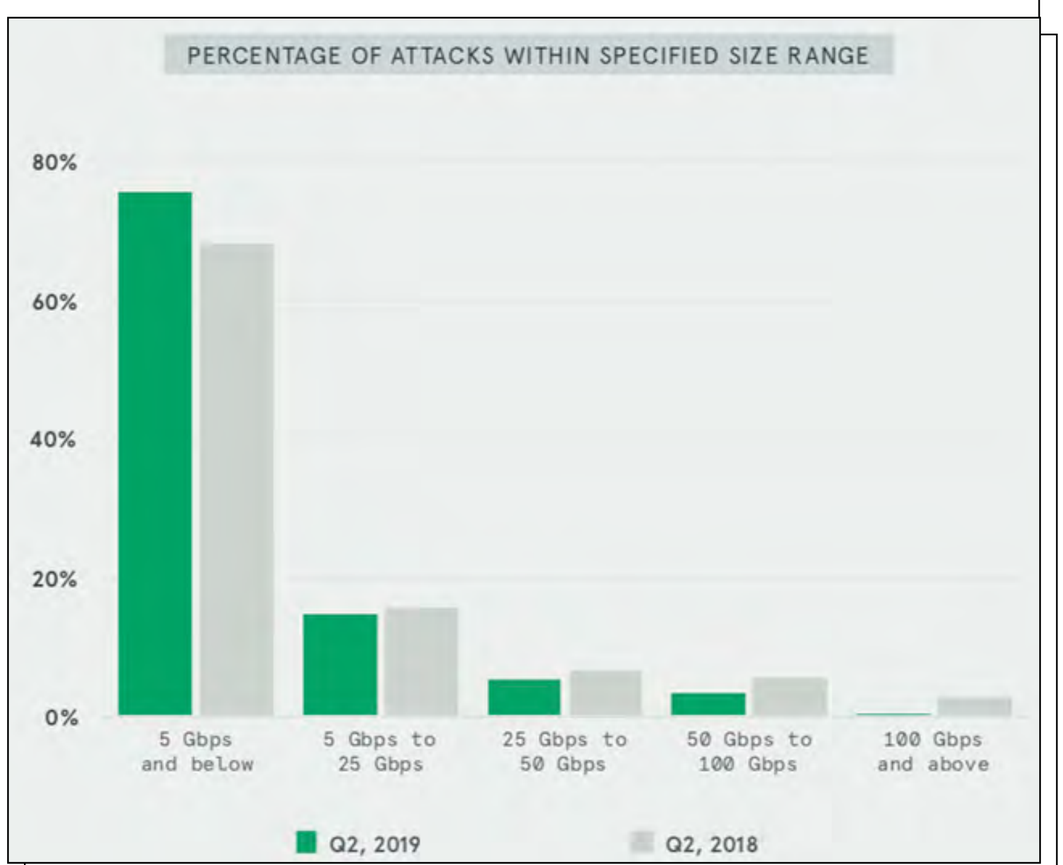
The number of DDoS attacks might be getting higher, but they are not all massive nor do they always trigger DDoS defenses. In fact, small-scale DDoS attacks are becoming more frequent and sophisticated, according to new research from Neustar's SOC.

According to the company's Q2 2019 Cyber Threats and Trends report, between April and June of this year, over 75 percent of all attacks mitigated by Neustar were 5 Gbps or less, while large attacks – those of 100 Gbps and over – decreased by 64 percent.

DDoS attacks have long been considered overwhelming threats and are traditionally associated with high rates of traffic. Such attacks do continue to take place, but smaller and more carefully targeted incursions are growing in quantity, intensity and duration.

Such attacks do not seek to saturate the network link – and draw unwanted attention in the process – but to degrade or disable specific infrastructure within the target. Such lower volume incursions may enable the perpetrator to get in and get out unnoticed or allow the attack to continue for quite a long time undetected. In fact, the longest duration for a single attack in Q2 was nearly two days.

These small attacks pose a significant threat, as they fall below the typical threshold that enterprises with a "detect and alert" DDoS mitigation strategy might employ. An attacker could therefore affect targets ranging from infrastructure to individual servers with relative impunity.



Organizations are employing cyber-resilient strategies in new ways

Wipro released its 2019 State of Cybersecurity Report, which highlights the rising importance of cybersecurity defense to global leaders, the emergence of the CISO as a C-Suite role, and an unprecedented focus on security as a pervasive part of the business operations.

The study found that one in five CISOs are now reporting directly to the CEO, 15% of organizations have a security budget of more than 10% of their overall IT budgets, 65% of organizations are tracking and reporting regulatory compliance, and 25% of organizations are carrying out security assessments in every build cycle. In addition, 39% of organizations now have a dedicated cyber insurance policy. All of these points showed dramatic increases from previous years.

49% of all risky online transactions come from mobile devices

About half of all risky online transactions appear to be coming from a mobile device, according to iovation. Specifically, in the first half of 2019 49% of all risky transactions came from mobile devices, up from 30% in 2018, 33% in 2017 and 25% in 2016. Iovation came to this conclusion by analyzing the 30 billion online transactions it evaluated for fraud from January 2016 to June 30, 2019.

“Fraudsters are like chameleons. They are always adapting their tactics to make it look like they’re legitimate customers,” said iovation’s Senior Director of Customer Success, Melissa Gaddis. “With well over half of all transactions now coming from mobile devices, our analysts increasingly see fraudsters either using mobile devices or making it look like their transactions are coming from mobile when in fact they are using a traditional desktop.”

Cybersecurity challenges for smart cities: Key issues and top threats

Urban population is on the rise worldwide and smart city development projects are harnessing the power of the Internet of Things (IoT) to develop more intelligent, efficient, and sustainable solutions. However, digital security investments in smart cities are severely lagging thus seeding the future vulnerabilities of the IoT ecosystem.

The Financial, Information and Communication Technologies (ICT), and defense industries will account for 56% of the US$135 billion projected total cybersecurity spend in critical infrastructure in 2024, finds global tech market advisory firm ABI Research.

The remaining 44% of the 2024 spend will be split between the Energy, Healthcare, Public Security, Transport and Water & Waste sectors – leaving them woefully underfunded and incredibly vulnerable to cyberattacks.

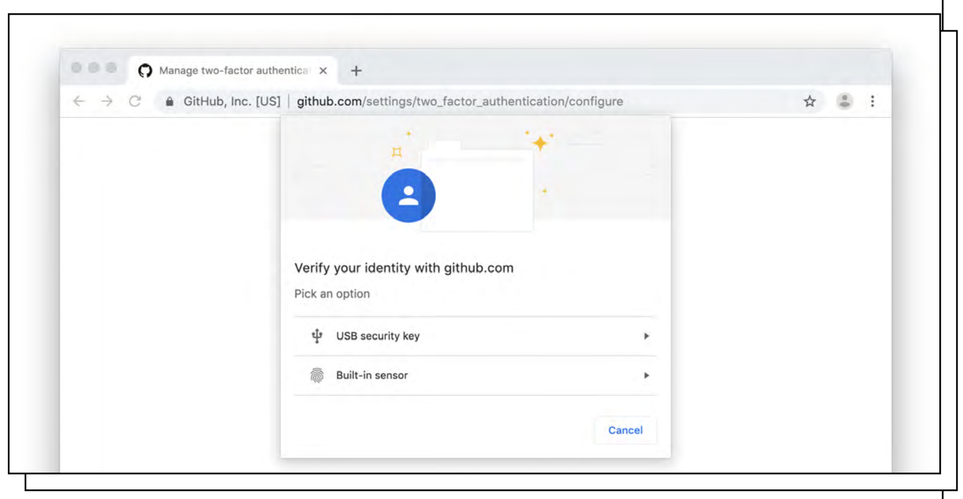
Most IT pros find red team exercises more effective than blue team testing

More than one-third of security professionals’ defensive blue teams fail to catch offensive red teams. The Exabeam survey, conducted at Black Hat USA 2019, also showed that 68% find red team exercises more effective than blue team testing, and more companies are practicing red over blue team testing.

The study showed that 72% of respondent organizations conduct red team exercises, with 23% performing them monthly, 17% quarterly, 17% annually, and 15% bi-annually. Sixty-percent conduct blue team exercises, with 24% performing them monthly, 12% quarterly, 13% annually, and 11% bi-annually.

The fact that so many organizations practice these exercises monthly speaks volumes about their maturity and dedication to fortifying their security posture. Not only do more organizations practice red team testing, but 35% of respondents claim that the blue team never or rarely catches the red team, while 62% say they are caught occasionally or often. Only 2% say they always stop the red team, emphasizing that organizations must constantly evaluate and adjust their security investments to keep up with today’s adversaries.

GitHub announces wider array of 2FA options, including security keys and biometrics



GitHub has started supporting the Web Authentication (WebAuthn) web standard, allowing users to use security keys for two-factor authentication with a wide variety of browsers and devices.

GitHub users have had the ability to additionally protect their accounts by switching on 2-factor authentication since 2013, but the choices were limited to receiving the second factor via SMS or getting it from a Time-based One-Time Password app such as Google Authenticator, Duo Mobile or Authenticator.

Later, they got the option to use physical security keys as GitHub began supporting the experimental U2F API for Chrome, but it was limited. With WebAuthn support in place, they can now use security keys with:

- Windows, macOS, Linux, and Android: Firefox and Chrome-based browsers
- Windows: Edge
- macOS: Safari (currently in Technology Preview but coming soon to everyone)
- iOS: Brave, using the new YubiKey 5Ci.

Five vendors accounted for 24.1% of vulnerabilities in 2019 so far

Risk Based Security reported today that VulnDB aggregated 11,092 vulnerabilities with disclosure dates during the first half of 2019, with CVE/NVD falling behind by 4,332 entries, according to their 2019 Mid-Year Vulnerability QuickView Report.

Five major vendors accounted for 24.1% of those vulnerabilities in 2019 so far. Further analysis reveals that 54% of 2019 vulnerabilities are web-related, 34% have public exploits, 53% can be exploited remotely, and that 34% of 2019 vulnerabilities do not have a documented solution.

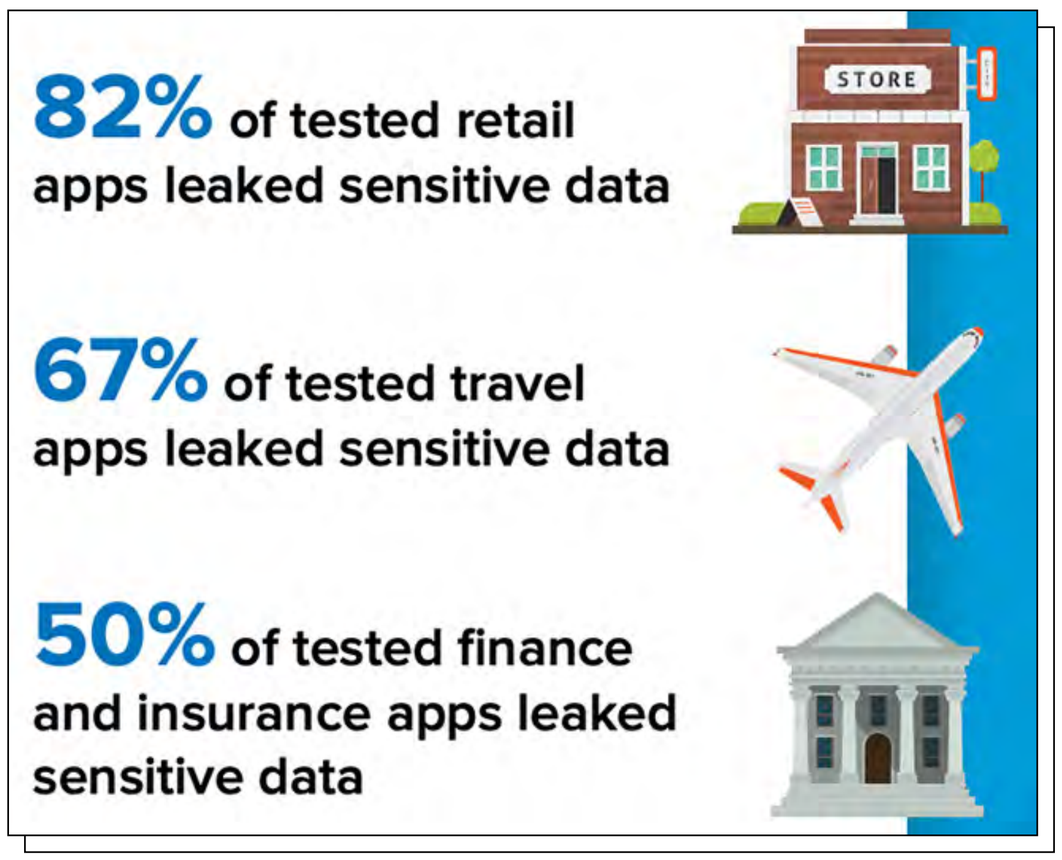
“34% of vulnerabilities do not have a solution, which may be because vendors are not patching. This can occur when the researcher has not informed the vendor, so they don’t know about the vulnerability,” commented Brian Martin, Vice President of Vulnerability Intelligence at Risk Based Security.

“Additionally, if an organization is using vulnerability scanning, they may simply not know about all of their assets. For example, if they are not scanning their entire IP space, or are using a scanner that is unable to identify 100% of their assets, then devices and servers may go unpatched.”

Organizations that scan applications in production have a reduced risk of being breached

Despite a significantly increased focus on application security testing, remediation rates for vulnerabilities continue to shrink, according to WhiteHat Security. Key findings of the firm's latest report include:

- The effort required to secure the rapidly growing volume of existing and new applications is overwhelming already short-staffed teams.
- AppSec investment is unbalanced across development, security and operations.
- Organizations that scan applications in production have a reduced risk of being breached.
- Organizations that embed security in DevOps are able to reduce risk, reduce cost and improve time to market.
- Embeddable components in the software supply chain account for 1/3 of all AppSec vulnerabilities.



Digital transformation helps companies work smarter yet makes them vulnerable to breaches

While digital transformation helps companies work smarter, there is a risk that the ongoing digitization may unlock a host of security vulnerabilities that can cost companies money, time, intellectual property, and customer trust, according to a Canon survey. All organizations surveyed across a range of verticals experienced an alarming amount of cyber threats over the past year.

Malware and ransomware:

More than one-third of respondents consider malware and ransomware a first priority threat. Yet, 25% of respondents say that employees have limited to no security awareness, nor do they understand their role in prevention.

Compromised devices:

In today's digital age, and with remote working trends on the rise, 21% of surveyed IT decision-makers rate compromised devices as a priority threat. Respondents then rank data security, network security, and user authentication & ID management as the top three most relevant technologies to help counteract this threat.

Social engineering:

The human factor is a persistent threat. In fact, survey respondents consider malicious insiders (30%) and human error (25%) to be the two top threat sources.

Attackers use large-scale bots to launch attacks on social media platforms

Social media sites have become lucrative targets for criminals looking for quick monetization. More than half of logins (53%) on social media sites are fraudulent and 25% of all new account applications on social media are fraud, according to the Q3 Fraud and Abuse Report by Arkose Labs.

According to the report, the U.S., Russia, the Philippines, UK and Indonesia have emerged as the top originators of attacks, with the Philippines as the single biggest attack originator for both automated and human driven attacks and the U.S. a distant second.

From account takeover attacks, to fraudulent account creation attacks, to spam and abuse, social media platforms see a variety of attacks from bots as well as organized malicious humans. However, more than 75% of attacks on social media are automated bot attacks.

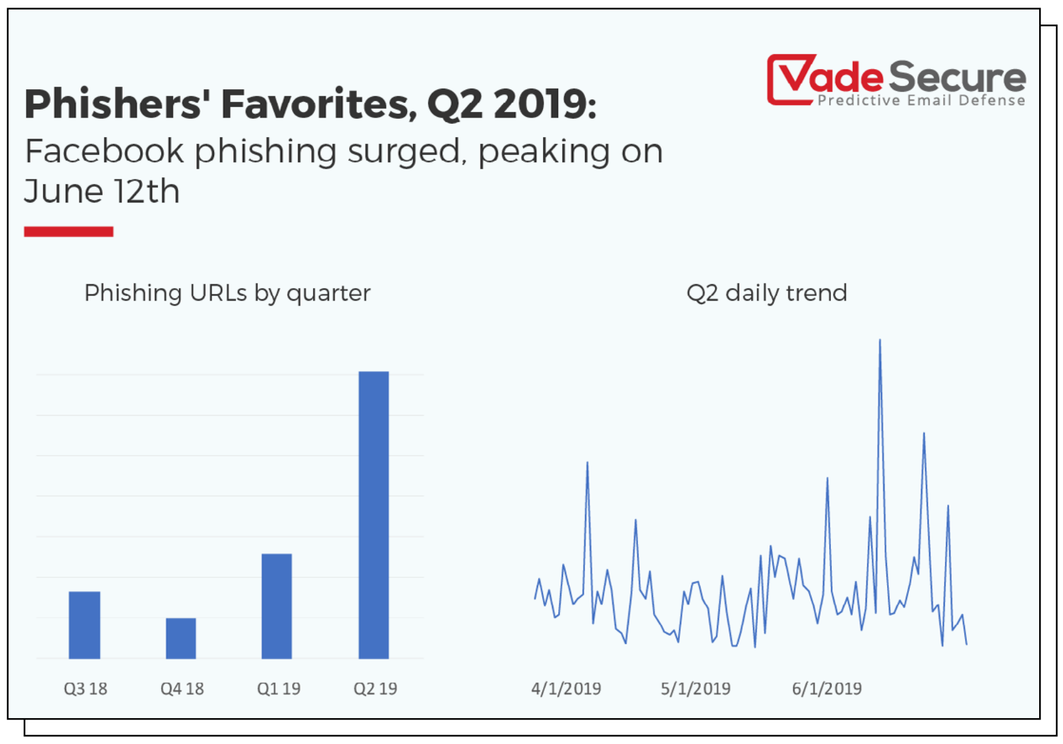
Unlike other industries, account takeover attacks are more common for social media, with logins twice as likely to be attacked than account registrations. This is driven by the fraudsters looking to harvest rich personal data from the accounts of legitimate users.

Facebook phishing surges, Microsoft still most impersonated brand

Vade Secure published the results of its Phishers' Favorites report for Q2 2019. According to the report, which ranks the 25 most impersonated brands in phishing attacks, Microsoft was by far the top target for the fifth straight quarter.

There was also a significant uptick in Facebook phishing, as the social media giant moved up to the third spot on the list as a result of a staggering 176 percent YoY growth in phishing URLs.

"Cybercriminals are more sophisticated than ever, and the ways they target corporate and consumer email users continued to evolve in Q2," said Adrien Gendre, Chief Solution Architect at Vade Secure. "Microsoft Office 365 phishing is the gateway to massive amounts of corporate data, while gaining access to a consumer's Facebook log-in information could compromise much of their personal, sensitive information. The fact that we saw such a significant volume in impersonations of these two brands, along with the coinciding new methods of attack, means that virtually all email users and organizations need to be on heightened alert."

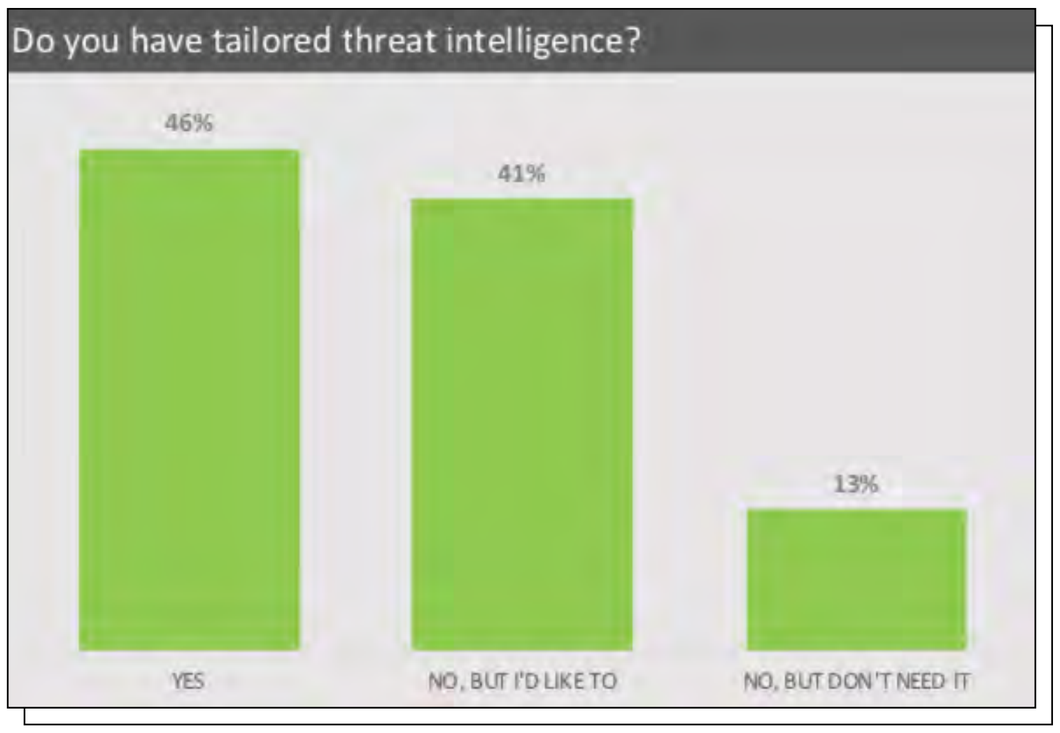


Automation, visibility remain biggest issues for cybersecurity teams

Organizations still do not have necessary levels of automation or visibility within their cyber terrain, especially as security stacks grow and are underutilized, Fidelis Cybersecurity's annual State of Threat Detection Report has shown.

Without automation to gather data and give context to security incidents, or visibility to root out threats hiding in the network, organizations' overall levels of risk increase while their confidence suffers.
Of the 300 respondents – CISOs, CIOs, CTOs, architects, engineers, and analysts across the finance, healthcare, public sector, federal industries – 57 percent shared that a lack of automation was a pressing concern for their organization, making it the top priority. This was closely followed by a lack of visibility, which had a pressing impact on 53 percent of organizations.

Most organizations are adding more point solutions, dealing with higher levels of network traffic, and working with more connected devices than ever according to the research. Yet often this is done in an urgent and reactive manner, without the necessary time and training to understand the full capabilities of the solution or assurance that they full integrate with the security stack for full interoperability. The result? Major security gaps and underutilized stacks.



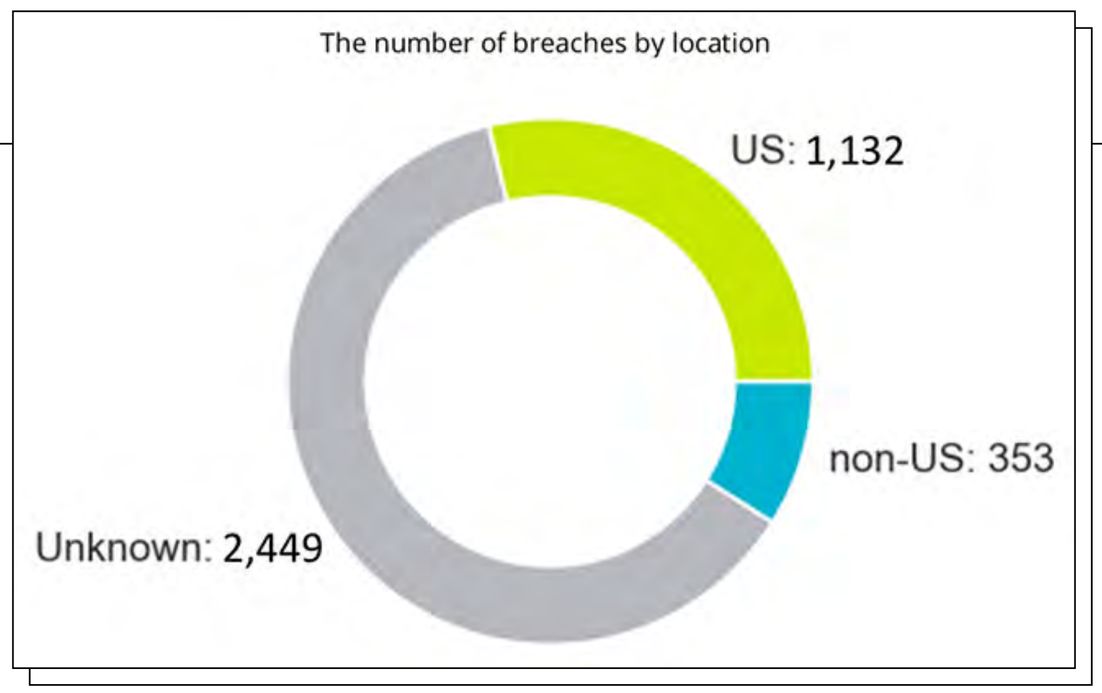
3,813 breaches were reported through June 30, exposing over 4.1 billion records

The number of reported breaches has gone up by 54% and the number of exposed records by 52% compared to the first six months of 2018 according to the 2019 MidYear QuickView Data Breach Report, released by Risk Based Security.

The research shows that eight breaches reported within Q1 and Q2 of 2019 accounted for 3.2 billion records exposed; three of these being among the largest breaches of all time.

The key findings state that The Business Sector accounted for 67% of reported breaches, which continues the trend observed in the Q1 2019 report. From these breaches, further analysis states that The Business Sector was then responsible for 84.6% of records exposed.

When asked about her observations on this activity, Ms. Goddijn commented, “Quarter after quarter the pattern has repeated itself. The vast majority of incidents are attributable to malicious actors outside an organization. Unauthorized access of systems or services, skimmers and exposure of sensitive data on the Internet have been the top three breach types since January of 2018. However, insider actions, both malicious and accidental, have driven the number of records exposed.”



Threat actors are adapting and switching their operations strategically and technically

Cybercrime campaigns and high-profile advanced persistent threat groups are shifting how they target victims and focusing more on intricate relationships with “secure syndicate” partnerships to disguise activity, according to the latest 2019 Cyber Threatscape Report from Accenture.

“Over the past year, cybercriminals have continued to test the resilience of organizations by layering attacks, updating techniques and establishing new, intricate relationships to better disguise their identities, making attribution more difficult to pursue,” said Josh Ray, a managing director at Accenture Security.

“Organizations should understand the tangible elements, or the bread crumb trail left behind, which can help reveal the motivations, operational procedures and tool use, to create a profile of the adversary. This process is critical for organizations to understand so they can proactively be involved in properly allocating resources and improving their security posture to avoid becoming cybercrime’s next victim.”

From imaging to monitoring systems, infusion pumps to therapeutic lasers and life support machines, medical devices are used to improve and streamline patient care.

Unlike other critical IT assets, connected medical devices are hardly visible in their native IT control systems.

Healthcare's blind spot: Unmanaged IoT and medical devices

AUTHOR_ Zeljka Zorz, Managing Editor, (IN)SECURE Magazine

Many of these are networked and they can be found everywhere in today's hospitals. Depending on who you ask, in the U.S. there are, on average, either a handful or between 10 to 15 connected devices per bed and keeping an eye on them is a difficult.

"Our data shows that hospitals on average have lost track of 30% of their networked medical devices, making it much harder to protect them against hackers. This is particularly concerning

because some 61% of all medical devices on a hospital network are at cyber risk and can be compromised by malicious attackers seeking to steal data, harm patients or ransomware," says Motti Sorani, CTO of medical cybersecurity provider CyberMDX.

The (security) problem with connected medical devices

Unlike other critical IT assets, connected medical devices are hardly visible in their native IT control systems, Sorani explained.

> *In an increasingly digitized world, protecting everything equally is not an option.*

"The IT teams often cannot even tell how many medical devices are connected, or their type, and they lack critical insight of the devices cybersecurity risk status, threats and vulnerabilities. Even more shocking, most hospitals lack the visibility to determine whether medical devices have been hacked."

And they are getting hacked and/or impaired, by hackers who are after information (personal, healthcare and financial data of patients and employees), money (mostly through ransomware and cryptocurrency mining), disorder (terrorists or "hacktivists"), or want to conscript new devices into their botnets.

"WannaCry, NotPetya, Orange Worm and botnets attacked medical and IoT devices because they are easy targets. Just last month the newly deployed Silex malware started bricking IoT devices, wreaking havoc everywhere, including the healthcare sector. And we hear of hospitals around the world getting hit by ransomware nearly every week," he pointed out. Real-world repercussions are many: hospital shutdowns, compromised patient care, regulatory infractions, potential lawsuits and the loss of a hospitals' good reputation.

Unfortunately, there isn't much patients can do when it comes to securing medical devices or their information.

In the U.S., HIPAA was created to protect (among other things) the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. But that's not nearly enough.

"All stakeholders involved must join together with renewed vigor to create more guidelines, regulations, and oversight," Sorani opined, and said that the same goes for the cyber protection of medical devices: hospitals, device manufacturers, security providers, and regulatory bodies must collaborate to set higher standards for security.

Preparing for the future

The future holds in store an even greater number of IoT devices deployed everywhere, and that includes wellness and health-assisting IoT devices.

These technological advances will surely improve patient care – once the patient care model is reinvented to take advantage of wearable health technology and telemedicine – but will also bring new risks.

"If we judge by the recent healthcare attacks – ransomware downing the systems in two Ohio hospitals, phishing attacks that breached 21,000 patient records in Minnesota, the enormous SingHealth data breach – no healthcare organization can hope to be overlooked in the long run," he noted.

"While many attacks are launched by lone wolves or small-time criminal affiliates, bigger attacks are usually performed by well-organized groups, often acting on behalf of nation-states. Given the global political situation, it's likely these types of attack will become bigger, bolder and more frequent."

Advice for healthcare CISOs

In an increasingly digitized world, protecting everything equally is not an option and HTM professionals must prioritize in order to focus mitigation efforts on more urgent needs and/or highest returns.

"Healthcare CISOs must gain visibility into their entire fleet of devices and incorporate the IoTs and medical devices into their cybersecurity program. They should look at solutions that could help them to automate, provide panoramic visibility into each device, and take control of them. Hospitals must deploy technology that not only identifies a security problem, but also solves it – from discovery and detection, to risk assessment and prevention," Sorani says.

It's also important for healthcare organizations to build cybersecurity strategies that cross multiple departments and functions.

"A cultural shift is required – one that breaks down silos between HTM professionals, IT and IS (and even the silos within those departments)," he added.

What the education industry must do to protect itself from cyber attacks

AUTHOR_ Charlie Sander, CEO, ManagedMethods

Data breaches show no signs of slowing down and companies across many industry verticals fall victim to what now seems to be a regular occurrence.

Most attention around data breaches is on the commercial side, with Capital One being the recent high-profile breach, compromising the personal information of more than 100 million people. However, the education sector is proving to also be an attractive target.

> *The start of the school year means millions of students and staff members will return to a school's cloud environment.*

This summer made it evident that K-12 school districts, higher education, and even commercial companies working with educational institutions are at risk. Notably, the state of Louisiana declared a state of emergency following an attack that disabled computers at three school districts. And it's not just a problem in Louisiana — schools nationwide are being targeted by hackers.

On August 2, the K-12 Cybersecurity Resource Center's K-12 Cyber Incident Map reported its 533rd publicly disclosed cyber incident, which means the number of data breaches against K-12 school districts in 2019 has already surpassed 2018's total. With four months still to go until the end of the year and the 2019-2020 school year beginning, school districts must take appropriate measures to protect themselves from the next attack.

Each year, more schools make the transition to the cloud and security falls further behind. The adoption of cloud technology in schools means that not only must security teams have the resources to monitor for suspicious and malicious activity from external threats, they must also

simultaneously be well-equipped to monitor for potential threats from within.

The start of the school year means millions of students and staff members will return to a school's cloud environment. It also means massive amounts of data will flow into, within and out of that environment. Computers, laptops, and cloud applications like Google G Suite and Microsoft 365 are now as essential to a school supply list as notebooks, binders and pencils. Teachers and staff members use these cloud-based productivity applications as much as they do email, spreadsheets and word processing. The fact is, schools today cannot function without these education-oriented cloud technologies and applications. At the same time, funding shortages mean that securing them is often not prioritized. But hackers are aware of this and schools should protect themselves moving forward.

Here are three ways to get the ball rolling:

Shift the focus to prevention, not mitigation

Most school districts have fewer than 2,500 students and don't have a staff member dedicated to handle cyber security incidents. Because of this, schools have become a target. But their mindset should shift from "if an attack happens" to "when an attack happens."

Many schools across the U.S. have made the transition — or eventually will — to running classroom and administrative operations in the cloud. The problem, however, is that securing the cloud applications in the new cloud environment has been an afterthought. This means schools are leaving student data vulnerable to identity theft, fraud, and other emerging threats.

By shifting the focus to secure applications and data before an attack happens, rather than after, schools and other organizations in the education market will be better prepared to protect students, staff, and operations against an external attack or internal incident.

Minimize internal threats

The increase in adoption of cloud applications means schools must also improve their security posture to prevent an internal incident. K-12 schools that have recently transitioned to the cloud, or are still making the transition, may not realize cyber security means more than securing a network with firewalls and gateways. It also means securing the data within the cloud environment — even when an individual and device physically leaves the premises.

The start of the school year means millions of students and staff members will return to a school's cloud environment.

Verizon's 2019 Data Breach Investigations Report found that nearly 32 percent of breaches involved phishing, 34 percent involved internal actors and that errors were causal events in 21 percent of breaches. Focusing on cloud application security as much as network or endpoint security will help minimize the internal threats that could occur throughout the school year and will help prevent sensitive data from leaving a school's environment.

For example, a member of a school's faculty could be at home and click on a phishing link in an email. That phishing link has now granted hackers access to the school's cloud environment. Attackers are then able to pass through any firewall and gateway schools have in place and can download and share any files they want. Most worrying of all, schools may never know the breach took place unless the hacker discloses it (as typically seen in a ransomware attack).

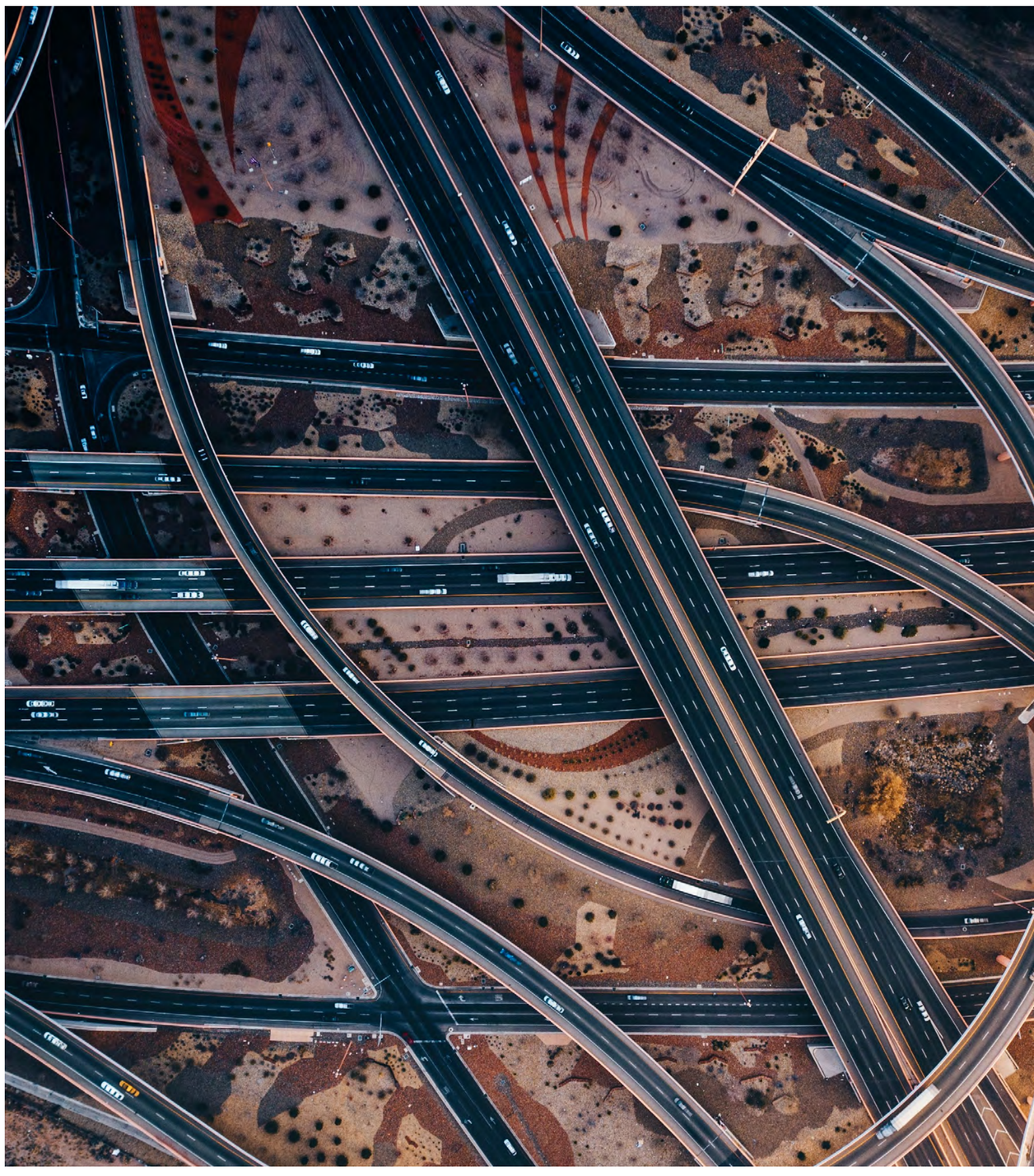
Make data loss prevention a priority this year

Educational institutions must fulfill data security and privacy requirements mandated by specialized laws and regulations such as the Family Educational Rights and Privacy Act (FERPA), the Children's Internet Protection Act (CIPA), the Children's Online Privacy Protection Act (COPPA), and the Health Insurance Portability and Accountability Act (HIPAA).

They must also protect their own organizational data, including the personal and financial data of their employees, and usually do it all without having huge security budgets.

When thinking about data loss prevention, most think of tools and solutions. But while data loss prevention tools can monitor user activity to detect improper or unusual behavior, preventing data loss goes much deeper. Institutions must educate staff and students on the most common types of human error and the various threats they may come across. They must also plan and documented processes to be better prepared and protected.

Attackers are becoming more sophisticated in their attacks and it's high time for schools to become more sophisticated in their defenses. Remember, security doesn't have to be expensive or complicated, but configuring protections correctly and monitoring for vulnerabilities and potential breaches is essential.



Solving security problems: Security advice for those with limited resources

AUTHOR_ Mirko Zorz, Editor in Chief, (IN)SECURE Magazine

In this interview, Mark Sangster, VP & Industry Security Strategist at eSentire, gives SMBs advice on how to minimize the risk of a data breach through better security practices, sets out priorities for a successful data security plan, and opines on the key challenges for the information security industry over the next five years.

Massive data breaches have unquestionably demonstrated that no organization, regardless of size, is immune to risky security practices. While large organizations have the financial resources to deal with the fallout of a data breach, SMBs are in a perilous position. What can they do?

Unlike larger large firms with comparable resources with which to protect client non-public information, small firms can find themselves trapped between cyberattacks like ransomware that don't discriminate based on the size of the firm, and regulators who are indifferent to your size when investigating a potential violation.

A 90-day snapshot of security operations statistics comparing large to small firms indicates relative volume of security incidents, but closer to par breaches and security events requiring immediate response. In this case, a large firm represents 500-750 employees working throughout 20 locations; whereas, a small firm is comprised of 25-50 employees at one location. The small firm generates 65,000 security traffic elements, that filter down to 20 incidents which led to one urgent incident that required immediate response. The large firm generated over 40 times more traffic, 325 security incidents (16 times more), and one escalation.

While the larger firm generates significantly more security traffic elements, as the security events were investigated, the ratio of escalated incident and incidents baring emergency response, moves closer

to one to one. Diving deeper, the data indicates that the emergency incidents were born of the same, industry-targeted attack. In other words, both the large and small firm were impacted and breached by the same targeted attack. Neither the criminals, nor their tools discriminate by the number of employees.

It's important that as firms expand their business in a growing environment of cyber threats, remember Sheriff Brody's advice: size does matter when you're going after big fish. As Sheriff Brody quips in Spielberg's 1975 blockbuster, Jaws, "You're going to need a bigger boat." Weigh then benefits and the risks. And recognize that there is chum in the water, put there by the criminals and the regulators alike. And be prepared for the behemoth that might bite your line.

Recommendations:

Inventory hardware, applications: Keep a register of all laptops, servers and applications. This should include cloud services such as Amazon EC2, Microsoft Office 365 or other document management services.

Identify and audit data and related obligations: By extension, you have the obligation to understand the legal and regulatory boundaries in which your clients operate, and to meet those requirements. Ensure you understand your obligations.

Engage an IT consultant: Managed Services firms can provide device management (updates and patching), along with basic system on-boarding and off-boarding processes. They can also help you encrypt devices and set up private networks to encrypt email and file transfers.

Establish cybersecurity and acceptable use policies: Leverage a consultant to build fundamental policies about the management, transfer and storage of client confidential information.

Protect sensitive data and avoid portable media: Avoid using media such as USB keys to store and transfer non-public information. USB keys are a main source of infection and are difficult to control if the data is not removed once the authorized use is complete.

Require encryption: Unfortunately, password credentials are routinely acquired by unauthorized users. For this reason, you should encrypt hard drives or devices.

Use VPN security: The best way to protect data in motion from such attacks is to use a Virtual Private Network (VPN) service. A VPN creates a secure and encrypted connection through which your data travels from you to the intended recipient. No information (including passwords) are transmitted in the clear. There are many low-cost and easily deployed VPN services.

Establish a records management policy (control and destruction): Determine how documents are stored, who has access and establish 'least privilege' with a 'need to know' attitude and consider how you securely destroy old documentation.

Establish a back-up system: Leverage an outsourced IT service to routinely back-up and then test backups to reduce the business disruption impact in the event of a cyber breach. Back-up are the best defense against ransomware attacks and avoid having to pay ransoms.

Consider cyber insurance: Engage an agent to weigh the cost and benefits of insuring your business against cyberattacks, and whether your business disruption, lost revenue or other non-cyber specific policies cover cyber incidents.

There are innumerable ways an attacker could gain access to sensitive data, which makes the process of building and running a strong security

architecture a considerable challenge. How can organizations better understand an attacker's mindset, motivations, and tactics to help them with their defense efforts?

Thinking like law enforcement, mean, motives and opportunities hold relevant when preparing to protect a business from cyber criminals. Criminals use lures and messaging tailored to your business, and often use your own tools against you to defeat defenses.

Opportunistic attacks like transactional ransomware is waning as criminals shift to more lucrative targets. Through broader attacks, they have identified businesses more likely to pay instead of suffering the consequences of a breach, public operation disruption or repetitional damage. Now we see phishing lures designed to peak the interest of the recipient. And they are designed to infiltrate the business and abscond with higher value assets, rather than smaller quick financial returns.

Moreover, and perhaps most concerning, criminals like to 'live off the land', exploiting your own vendor services and operating systems tools. Our research indicates that of more than 650 respondents, over 44% had suffered a material breach as a result of their supplier. And more disturbingly, only 15% of these breaches were reported by the vendor.

In many cases, they use a compromised user account to use remote administration tools (RAT) or the remote desktop protocols (RDP) built into all operating systems. Their activity looks like normal administrative tasks such as creating new users or changing user privileges, but at the microscopic level, the differences are evident and show a trend toward creating unauthorized users who can disable security systems, delete logs, and move through your network with impunity.

Much of this information is recorded and published by law enforcement agencies, and task forces called ISACs (Information Sharing and Analytics Centers) that focus on cyber events for core economic pillars such as banking, healthcare, law, transportation, and so on. These organizations offer public resources.

An expanding cybersecurity skills gap is creating issues for organizations of all sizes, and many of them don't have an adequate ability to detect and respond to threats in a timely fashion. How can overworked security teams overcome this challenge?

It's not finding the needle in the haystack. That's easier than dealing with the needle. The headline around the cybersecurity skills gap hides the real story. It's not simply the general shortage of experts, but it's a shortage of specific experts within the cyber community. Of top priority is the need for experts who can hunt for threats using a myriad of cyber sensors and logs, and also experts who know how to respond when they discover unauthorized activity.

There is no shortcut to truly automate cybersecurity. Artificial intelligence can greatly reduce false-positives (data that needs to be chased down to eliminate threats, but turn out to be innocuous or a false alarm), and orchestration tools can help streamline investigations and response, but the trick is combining technology, with experts and well tested processes. Time is money. The faster an event is stopped, the less it will cost the business in the long run.

Most mid-sized firms prefer focus on their business and partner with a vendor who can deliver services that are either too expensive to develop in-house or too difficult to staff. Managed detection and response services provide threat hunting and response services that can complement in-house expertise in network and logging management.

What advice would you give to a newly appointed CISO that needs to strike a balance between data use and the associated risks? What are the priorities for a successful data security plan?

IT and security are stressed by the opposing forces of the demand for competitive advantages through adoption of technology, and while mitigating, lowering or avoiding risks that could materially impact the business. The reality is that most if not all data is digitized and shared across an ever more distributed IT environment and scattered workforce.

Cybersecurity is a risk issue and not a IT practice. And CISOs need to speak the language of the Board and executives. It's critical to consider risk, align with the general counsel and provide technical information in a way that resonates with business leaders. The role of the CISO is to impact the quantifiable risk, with mitigation strategies so that business leaders can make an informed decision about spend and risk tolerance.

CISO top priorities:

- Regular cadence of annual planning, quarterly reporting to the board.
- Dashboard and flash communications that focus on regulatory changes, security performance, risk registry, and incident testing and results.
- Run 2-4 annual incident simulations based on most likely scenarios. Engage the board in their role and review findings.

CISOs and board alike can leverage public documents such as the National Association of Corporate Directors (NACD) Cyber Risk Handbook and the National Cyber Security Centre (NCSC) Board Toolkit for programs, dashboards and best practices.

What do you see as the key challenges for the information security industry over the next five years?

Budgets for security continue to grow, and in smaller firms, now garners the attention of senior management, the board, and even strategic investors. This is a blessing and a curse. The blessing is direct access to decision makers, resources and funds to run a security program. Perhaps an exaggeration, the curse is direct access and ever watching spotlight. It's important to proactively address security concerns, focus on risk not security tools, and engage the board in decision making rather than coming with hands out for more funds and headcount.

Attacks that leverage your own tools (living off the land) will increase and the subtlety of these attacks will provide almost perfect camouflage with which to hide in plain sight within your environment. This means controls must tighten, relying on multiple stages, and systems that look for a collection of anomalies instead of well know signatures and patterns. AI, behavioural analytics and user access controls will become paramount.

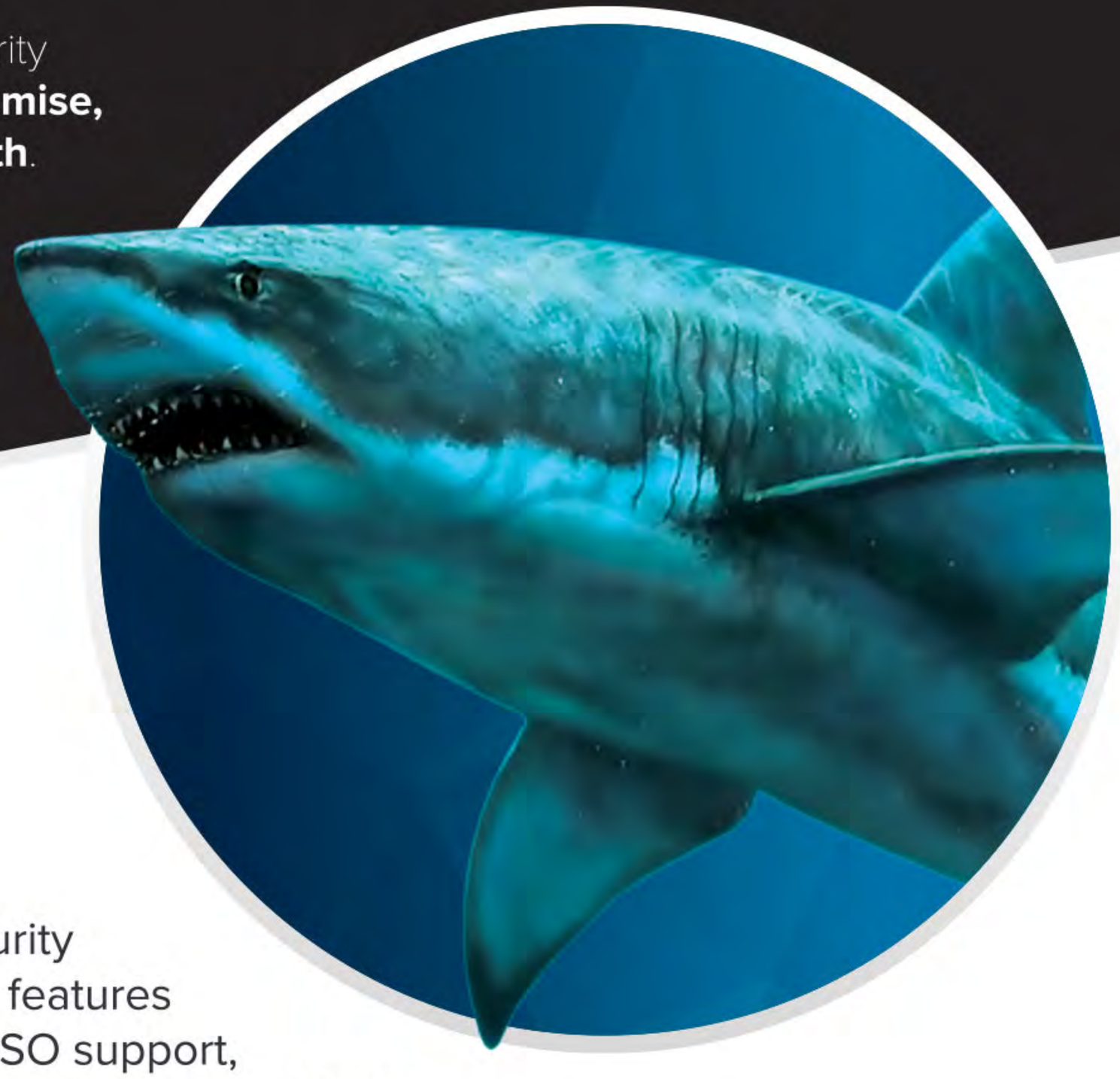
The consequences of breaches will continue to tighten the reins of accountability. Insurance firms will hones their actuarial data and demand heightened security. More claims will be rejected when the insurer thinks the claimant failed to meet basic security standards, and courts will treat cyber claims under tort law which means well understood damages, and the ability for plaintiffs to collect without proving damages. As in, the risk of damage associated with exposed data will be rough for courts to award settlements.

The adoption of emerging technology will accelerate shortening the window in which security professionals can access risk and deploy mitigation strategies. Interconnected and always connected (5G) devices will be pervasive and accelerate the drive for distributed workforces and perimeter less organizations.

netsparker

WEB APPLICATION SECURITY SOLUTION

Netsparker is a web application security solution that can be deployed **on premise, on demand or a combination of both**. Unlike other web application security scanners, that lack scalability, Netsparker was designed with enterprise in mind.

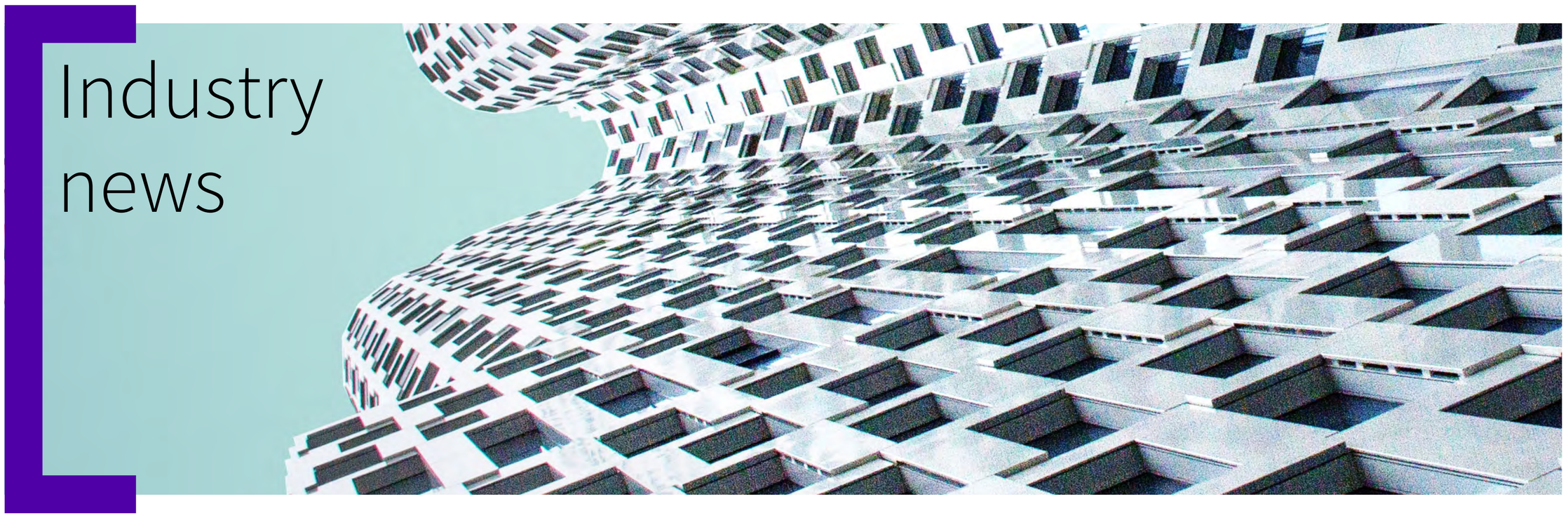


Proof-Based Scanning™

Netsparker's web application security solution is packed with enterprise features such as workflows, integrations, SSO support, 2FA support, and proprietary technology that confirms false positives. The combination of these features allows Netsparker to scale scanning from 100 to 1000's of websites in a short period of time.

The Walt Disney Company · U.S. Department of Homeland Security · McAfee · NASA · Microsoft · Coca-Cola · SAMSUNG · Skype · NFL

www.netsparker.com
info@netsparker.com
+1 415 877 4450
+44 (0)20 3588 3840



Industry news

YubiKey 5Ci: First security key designed with both USB-C and Lightning connectors

This unique dual-connector functionality makes the YubiKey 5Ci the perfect solution for consumers or enterprises looking for strong hardware-backed authentication across iOS, Android, macOS, or Windows devices. The YubiKey 5Ci is available at a retail price of $70 USD.

The YubiKey 5Ci can be used to secure the 1Password, Bitwarden, Dashlane, Idaptive, LastPass, and Okta iOS mobile applications along with additional services accessed through the Brave iOS browser app. Supported logins on the Brave browser include Bitbucket.org, GitHub.com, Login.gov, Twitter.com, and 1Password.com. Monkton Rebar and XTN also support the YubiKey 5Ci in their latest software development kits.

To support a growing ecosystem, Yubico continues to work with industry leading iOS applications and browser supported services through the Yubico Developer Program. Partners with anticipated YubiKey 5Ci app support include Dropbox, SecMaker, and others.

Authentication with the YubiKey 5Ci is also available over a USB-C connection, which is compatible with nearly every USB-C equipped laptop or mobile device, working with hundreds of applications and services listed in the Works with YubiKey catalog today. Some capabilities are not currently supported on iPad Pro models with USB-C ports.

BitSight Enterprise Analytics enables more effective risk management

BitSight Enterprise Analytics helps security and risk leaders gain insight into the impact of risk introduced at the organizational group level – from subsidiaries to business units and departments – enabling them to identify the areas of highest risk concentration within their organizations. The solution provides visibility into which groups have the biggest impact on their organizations' overall cyber risk posture and helps identify areas for security performance improvement.

Global Cyber Alliance releases AIDE, a cybersecurity development platform for IoT products

The Global Cyber Alliance, working with its partners, launched the Automated IoT Defence Ecosystem (AIDE), a first-of-its-kind cybersecurity development platform for Internet of Things (IoT) products.

AIDE enables small businesses, manufacturers, service providers and individuals to identify vulnerabilities, mitigate risks and secure IoT devices against the growing volume of threats to this interconnected environment.

A complementary resource to the AIDE platform is the GCA ProxyPot, a custom IoT honeypot solution developed by GCA, which is capable of replicating one IoT device across multiple IP addresses and physical locations to identify global attack risks quickly, efficiently and accurately. Together, the AIDE and ProxyPot platforms allow for organizations and individuals to have greater visibility into the types and scale of threats facing the IoT devices deployed into various environments, including smart cities and other smart ecosystems.

A new online tool monitors the state of internet routing security

MANRS Observatory is a new online tool that measures the level of networks' compliance to MANRS, a key indicator of the state of routing security and resiliency of the Internet. The tool aggregates data from a number of trusted third-party sources into a user-friendly online dashboard. This snapshot enables network operators to identify problematic areas to help them improve the security of their networks.

Attivo Networks' portfolio enhancements lock down endpoints so attackers cannot advance

Attivo Networks announced significant portfolio enhancements that effectively lock down the endpoint so that attackers cannot advance their attacks. These innovations include securing Active Directory and the ability to turn every endpoint into a network decoy. The company's ThreatDefend Detection Platform provides a comprehensive deception fabric that interweaves decoys, lures, and breadcrumbs throughout the network. By blending in seamlessly with the production environment, the deception fabric sets landmines and bait to derail attackers and alert on their presence.

400G Triton cyber warfare simulation tool can replicate any attack

Telesoft Technologies — a provider of cyber security technologies for high-density cyber environments, including network, government, and large organizations — has announced the release of Triton 400, a cyber warfare simulation tool which can replicate a myriad of adversarial attack methods.

Mimicking attacks from all over the world, Triton 400 utilizes a comprehensive understanding of frontline threat intelligence from around the globe to simulate natural and malicious traffic at unprecedented speeds for such a capability.

Taking a unified approach to security, Triton 400 provides a benefit to both red and blue teams. Red teams can attack infrastructure at a high rate with myriad threats from multiple vectors, doing everything in their power to penetrate the network. They can manipulate the method of attack to replicate selected threats and techniques against specific organizations and networks.

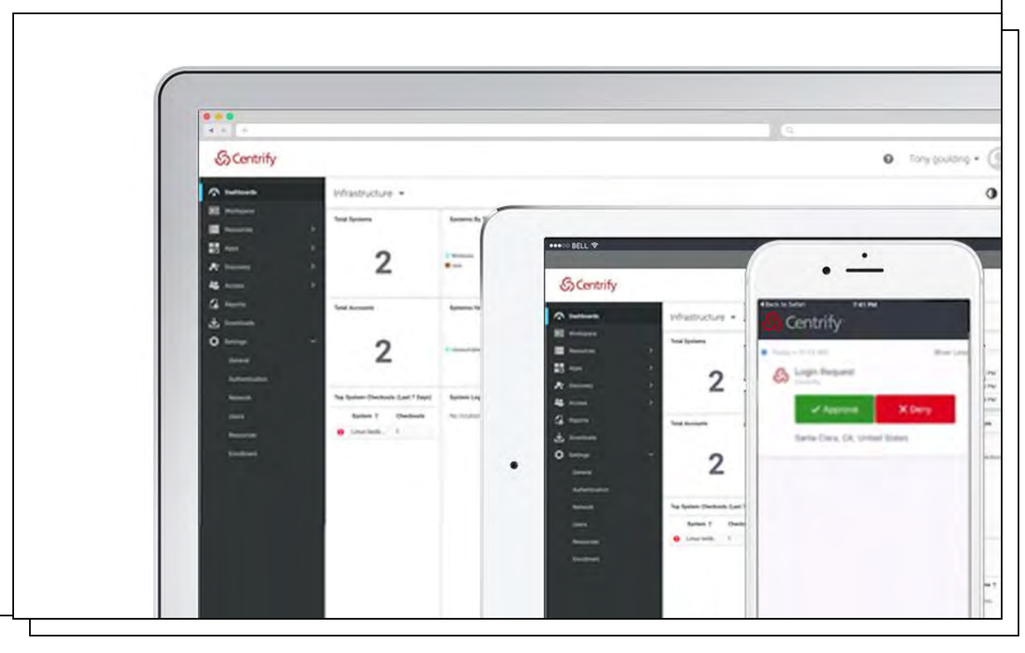
Triton 400 can replicate any type of attack, from password spraying and large-scale DDoS to AI poisoning, whilst also generating multiple simultaneous attacks — one as a smokescreen and the other malicious to challenge blue teams more than ever before.

WatchGuard's ThreatSync detects and remediates zero day threats and evasive malware

WatchGuard Technologies has announced major updates to its threat correlation and response platform, ThreatSync, with the latest release of Threat Detection and Response. These enhancements include accelerated breach detection, network process correlation and AI-powered threat analysis, enabling MSPs and the organizations they support to reduce breach detection and containment timeframes from months to minutes, automate the remediation of zero day malware and better defend against targeted, evasive threats both inside and outside the network perimeter.

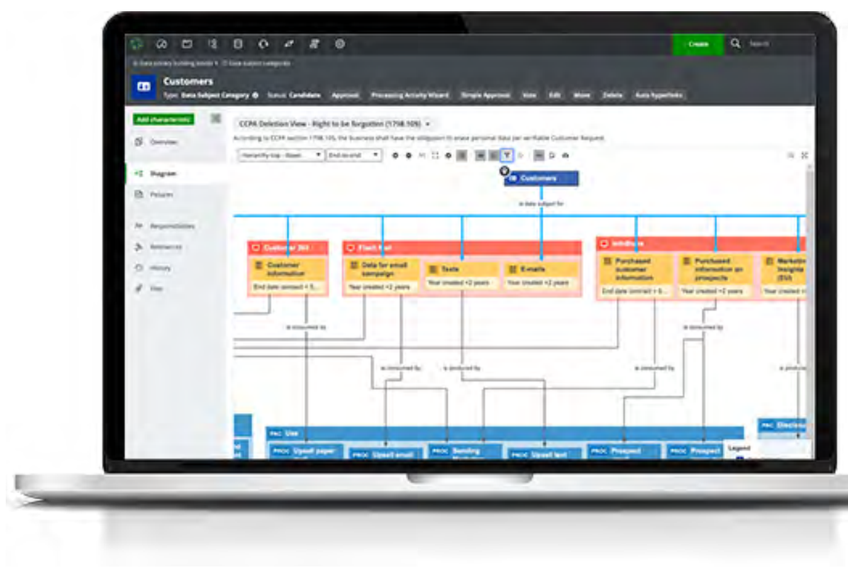
Centrify unveils free cloud-based PAM offering for organizations that do not have a password vault

Centrify announced a free cloud-based Privileged Access Management (PAM) offering for the more than half of organizations that do not have a password vault. Centrify's Free Tier Vault is available immediately in the AWS Marketplace, enabling organizations of any size to start controlling privileged access to critical systems and sensitive data in minutes, delivering PAM-as-a-Service.



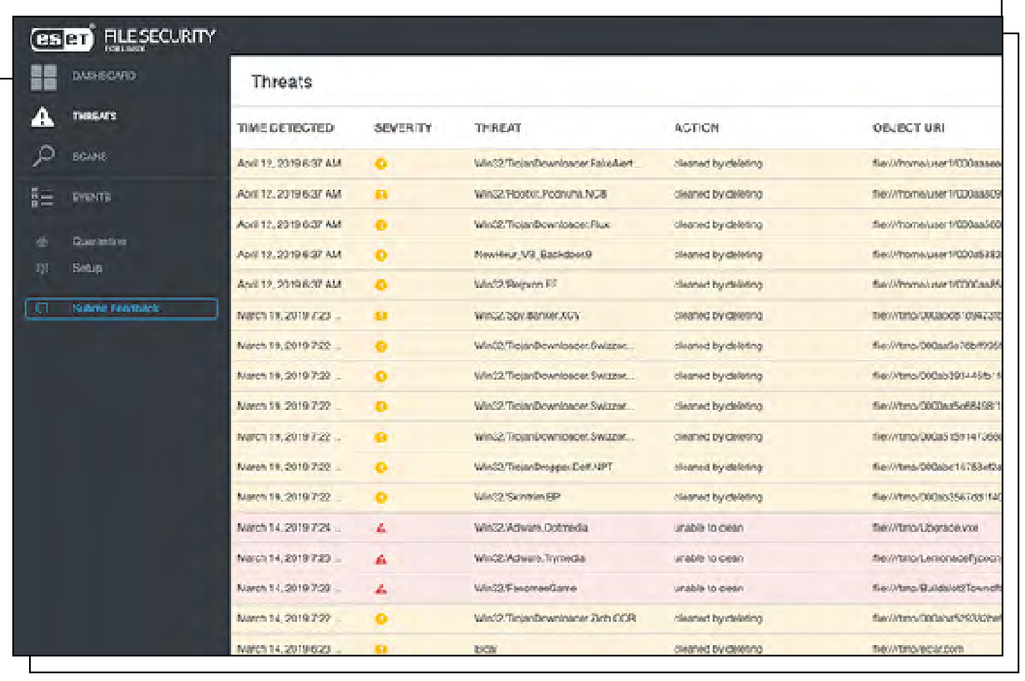
Collibra's new product enables a proactive approach to data privacy

Collibra Privacy & Risk is a new enterprise-grade product that will empower organizations to proactively manage personal data assets by enabling compliance with privacy regulations, helping to protect data, and unlocking new opportunity from insights. The latest addition to the Collibra platform, the new product includes modules for the CCPA and the GDPR and builds the foundation for a strong data culture that will be prepared for future regulatory requirements.



ESET unveils new version of File Security for Linux

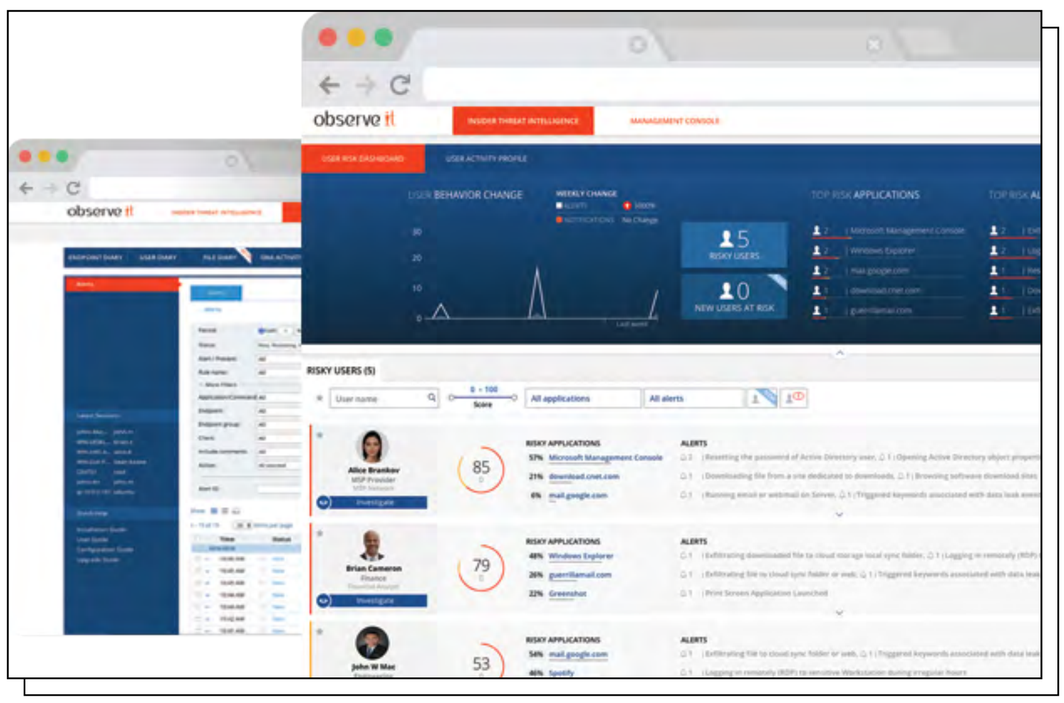
ESET File Security for Linux provides protection to organizations' general servers, network file storage and multipurpose servers. The software ensures the servers are stable and conflict-free in order to preserve system resources for vital tasks and avoid disrupting business continuity. Version 7.0 offers a host of advanced features, including real-time file system protection, tighter security and a real-time web GUI.



ObserveIT unveils crowdsourced insider threat analytics solution

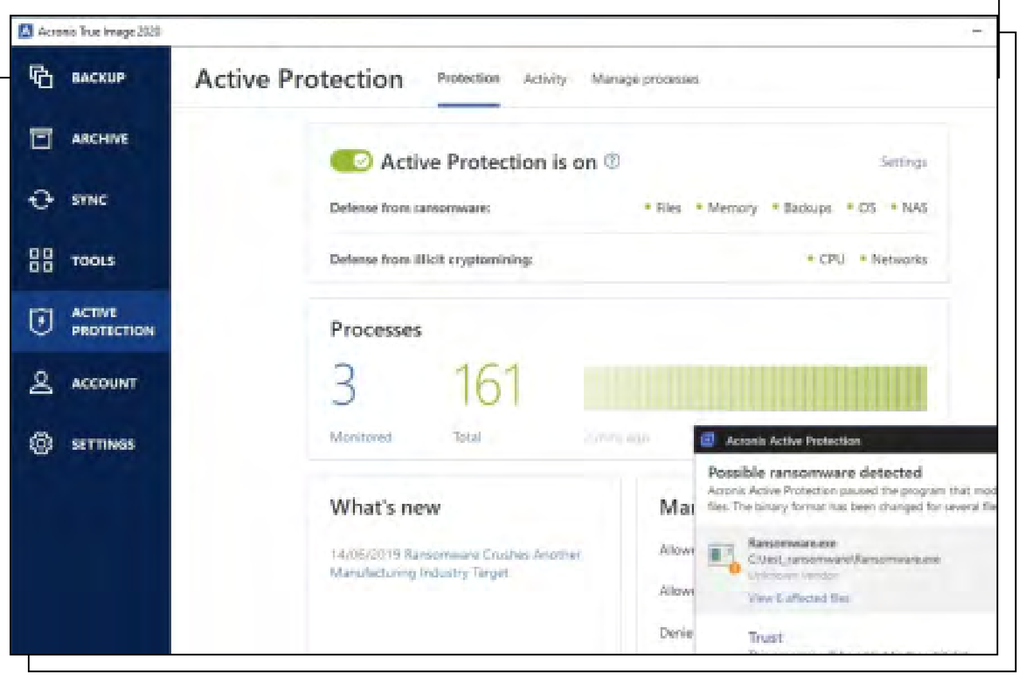
ObserveIT, the leading insider threat management platform with more than 1,900 customers around the world, announced the availability of an Insider Threat Analytics solution powered by crowdsourced industry insight.

This release advances ObserveIT's ability to analyze threat indicators using community-driven intelligence to help its growing customer base get ahead of potential threats and protect their most valuable assets. ObserveIT's Insider Threat Analytics capabilities address this by providing an additional layer of defense to protect against insider threats using the most comprehensive industry intelligence, allowing security teams to know the whole story and take action in minutes rather than days or weeks.



Acronis True Image 2020 replicates local backups in the cloud

Acronis True Image 2020 enables users to automatically replicate local backups in the cloud – making it the first personal solution to automate the 3-2-1 backup rule that data protection experts almost universally recommend. What's more, the Dual Protection replication feature is just one of more than 100 enhancements and new capabilities incorporated into Acronis True Image 2020 that are designed to further improve its performance, control, and security.

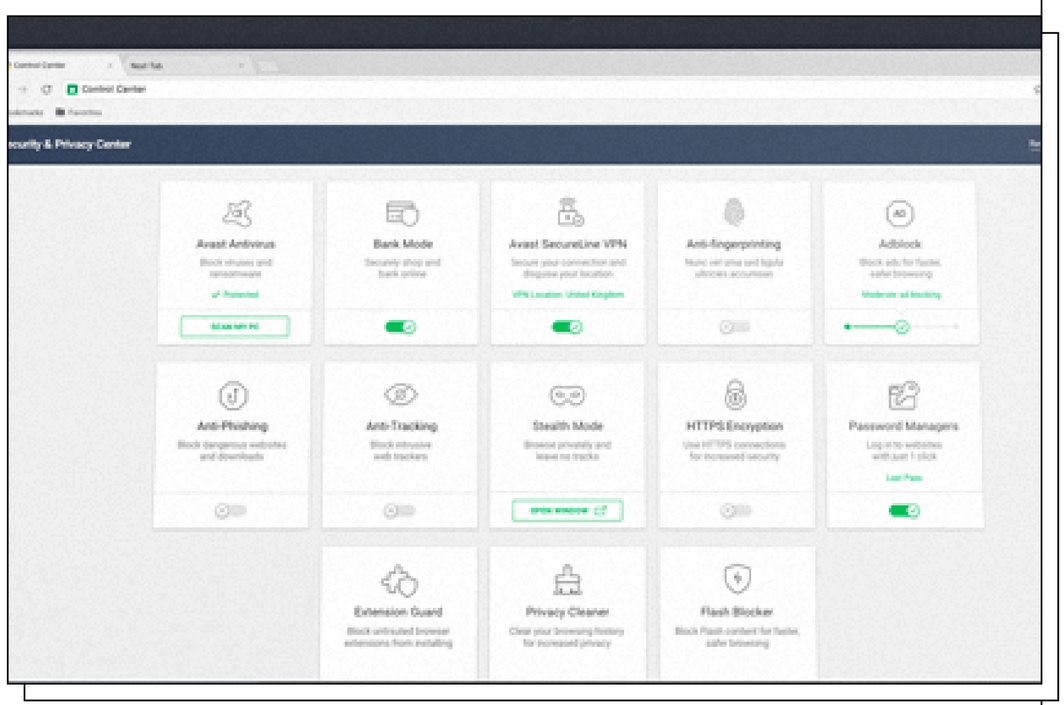


XebiaLabs expands its Software Chain of Custody reporting capabilities

XebiaLabs announced a major expansion of its Software Chain of Custody reporting capabilities. The Chain of Custody delivers crucial evidence about the entire software delivery pipeline; it proves what happened, when it happened, where it happened, and who made it happen. The XebiaLabs DevOps Platform version 9.0 introduces the first and only Release Audit Report that covers all release activities from end to end—at the push of a button.

Avast Secure Browser enhanced with built-in memory and battery-saving controls

Avast has introduced built-in performance and battery-saving enhancements in the latest release of Avast Secure Browser, code-named "Zermatt". Avast Secure Browser's Anti-Fingerprinting technology has been upgraded to protect user identities against advanced data gathering methods and tailored attacks by cybercriminals looking to exploit installed software modules.



Review: Specops uReset

AUTHOR_Vlatko Kosturjak, Security Researcher

Yes, it's 2019 and we still have to deal with passwords. They should be replaced or supplemented with multi-factor authentication as soon as possible, but it looks like they are here to stay, and their number keeps growing with the number of services we use. When it comes to password management problems in an organization, you have to think about the process that is put in place for when users forget their password. If the authentication process is difficult to bypass, attackers will try to take advantage of the password reset procedure.

Resetting passwords

The password reset procedure must be at the same security level as the authentication process (if not higher!) – there must be a way to securely reset passwords. This process needs to involve checking the identity of the user who requested a new password and is generating a new password.

Depending on the employee structure, the process of resetting passwords can be quite a challenging task for the helpdesk, as it can take some time which ultimately drives cost – IT support and user downtime.

Specops Software came up with a tool to help with and automate the password reset procedure in a secure way. Specops uReset is a Windows-based tool that plugs into the Active Directory authentication process and allows you to customize the level of security that your organization requires by extending various multi-factor authentication options to the password reset process.

The uReset concept

Specops uReset can be installed on Active Directory to automate the password reset procedure, which is carried out by using multi-factor authentication including various authentication methods from third parties. For example, you can configure it so that employees can self-reset the password via their mobile phone, via Gmail, or a Facebook account, and without needing to contact the helpdesk.

The product implements a number of ways for users to prove their identity, ranging from social identity providers (Facebook, Google, Twitter, GitHub, etc.) to authentication providers (Duo Security, Microsoft Authenticator, Google Authenticator). Other options include Mobile Code and Specops own methods (fingerprint and OTP) for the password reset procedure. Of course, the administrator can decide which service(s) and method(s) can be used to reset users' passwords, which can be extended not only to end-users but also to helpdesk users resetting users' passwords.

Users can reset their password via a web browser and via a reset link on the Windows login screen.

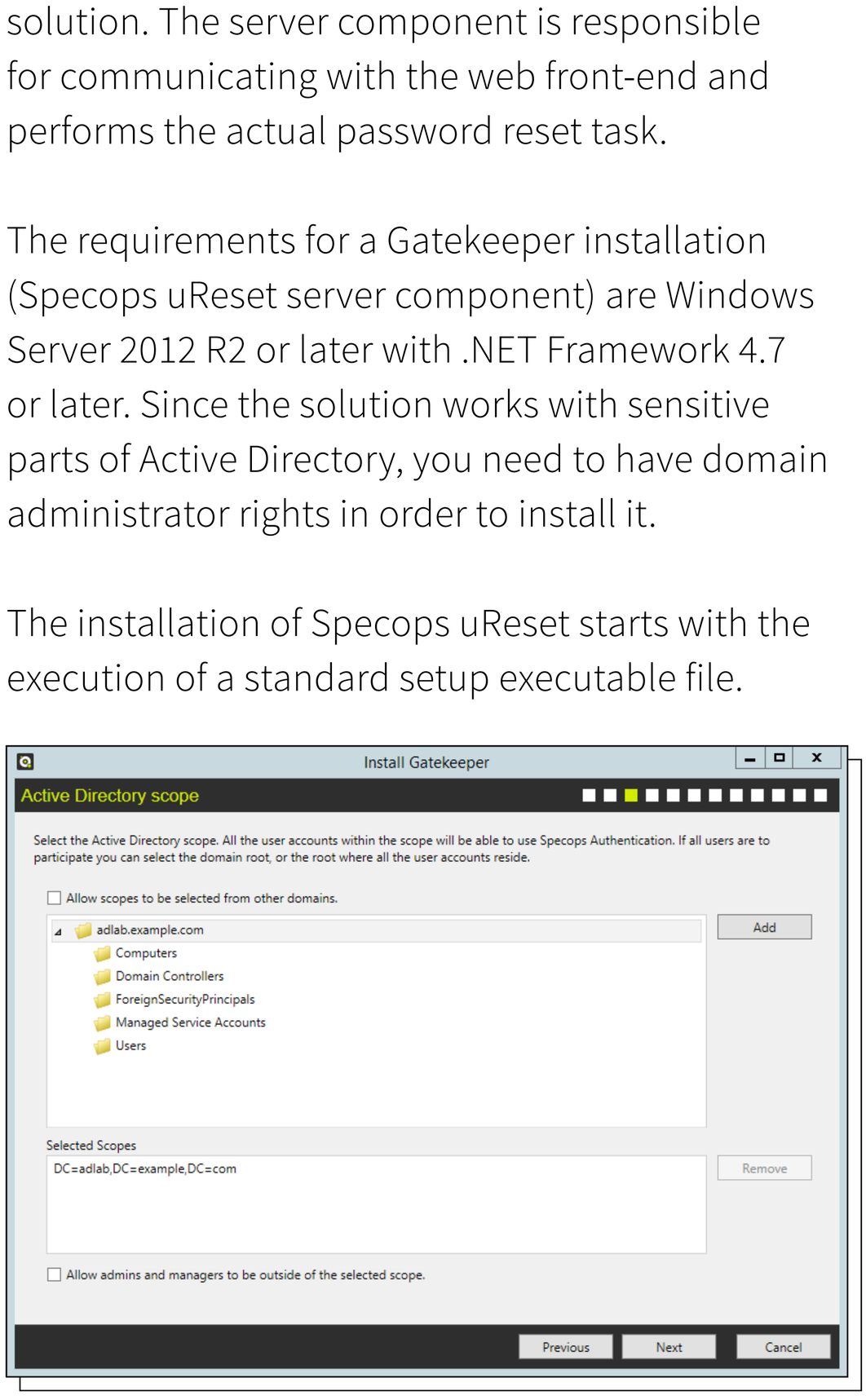
There is also the option to download the mobile application, which makes the entire process easier.

Installation

Specops uReset is a cloud solution. Still, you'll need to install a server component that will "talk" to the cloud. Installing a mobile application for your users is optional as there are different choices when it comes to resetting passwords. Users can self-reset the password by following the clear instructions on the web site of the cloud solution. The server component is responsible for communicating with the web front-end and performs the actual password reset task.

The requirements for a Gatekeeper installation (Specops uReset server component) are Windows Server 2012 R2 or later with .NET Framework 4.7 or later. Since the solution works with sensitive parts of Active Directory, you need to have domain administrator rights in order to install it.

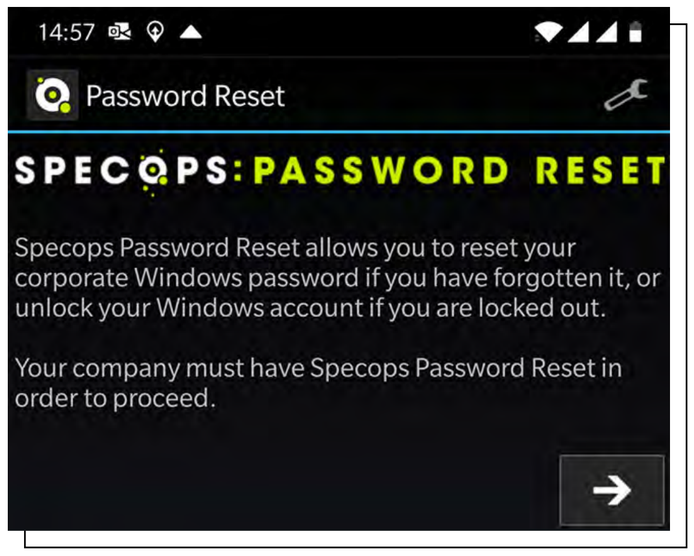
The installation of Specops uReset starts with the execution of a standard setup executable file.



THE INSTALLATION OF THE SERVER COMPONENT IS STRAIGHTFORWARD

For the test, we have installed a test Active Directory domain in an AWS cloud with a few testing servers as part of the domain. We have

populated users with different privileges and roles with the test script. We have set up the server component in less than five minutes by following the provided instructions. The most complicated step was to paste the authorization code that was obtained during the download of the setup file.

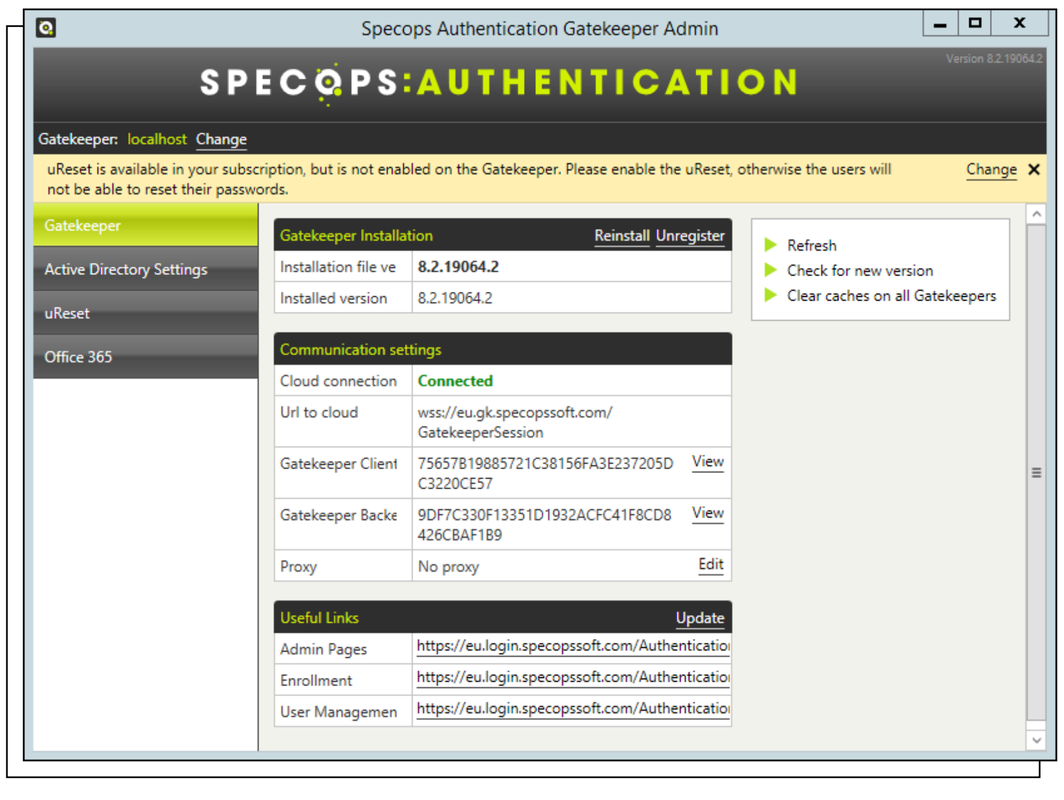


SPECOPS URESET ANDROID APPLICATION

Mobile applications can be installed from official application stores. Apps are available for iPhone and Android users.

Usage

Once installed, you need to go through the initial configuration process to adjust basic Active Directory settings. It is a standard Specops product configuration: configuration categories are on the left side, detailed items which can be modified are on the right side.



SPECOPS URESET SERVER CONFIGURATION

Once the server component is configured, the next step is to access the admin part on the provided website. There, you can configure password reset providers and methods to reset the password. Also, you can enroll users to the self-reset password service provided by Specops uReset.

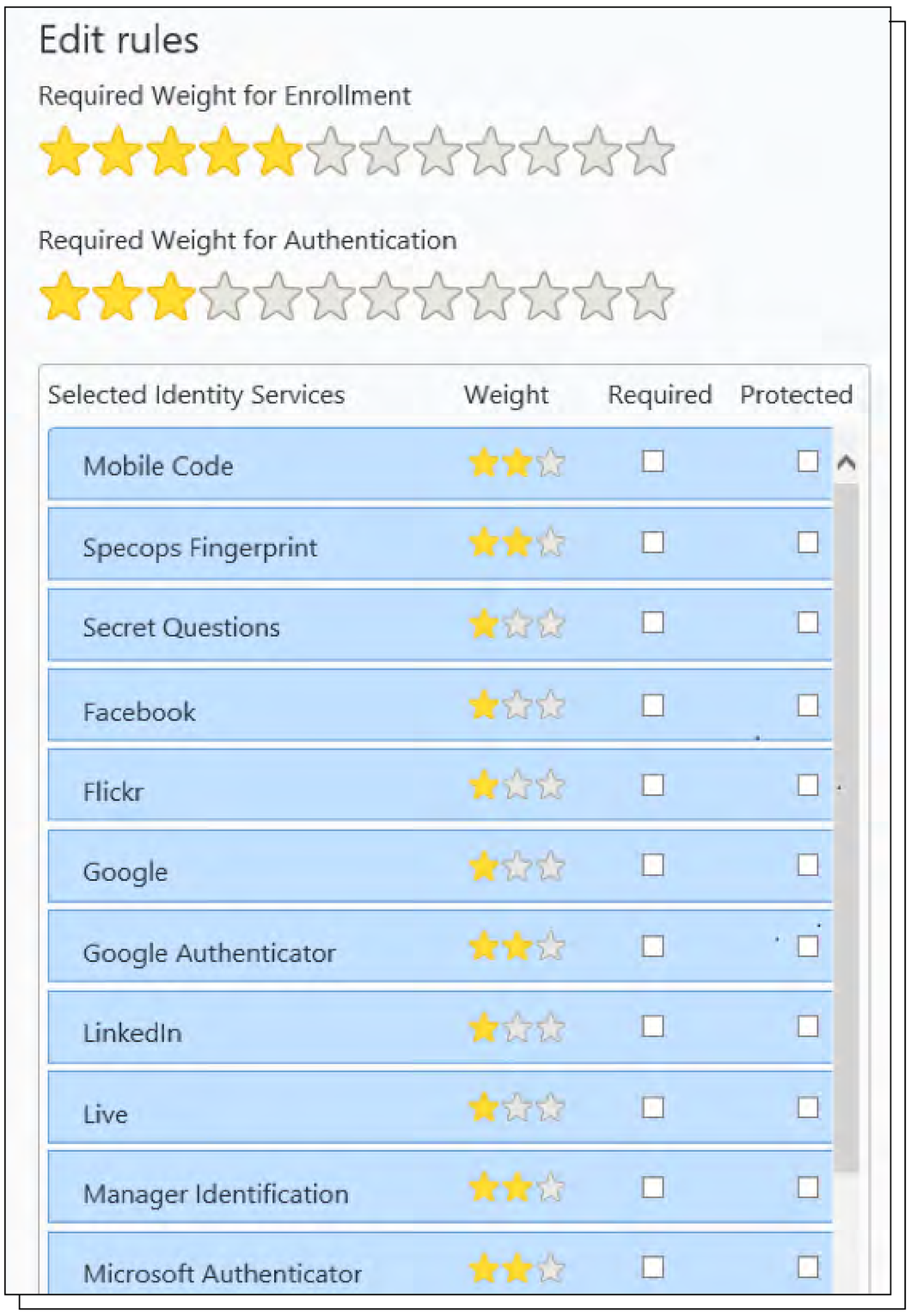
More on user enrollment

Note that some of the methods need additional configuration and some of them are ready to be used directly “out of the box”. The latter is possible if your Active Directory is already populated with the correct data for each user that will be given the password reset option. For example, the “Mobile” field should be populated with the correct mobile number of the user if you want to enable password reset via Mobile Code. Another example would be the “Manager” field, if the manager can identify the person.

You can also configure Symantec VIP this way, but you need to specify the LDAP attribute where the Symantec User ID is stored. A similar example is the “samAccountName” attribute for a reset if you want to provide a password reset option via the Duo Security solution.

Helpdesk workers will also appreciate this tool as they will not have to handle password reset requests on a daily basis.

Specops uReset is very flexible, so system administrators, together with their security department, can assign a specific value for each identity service, ultimately deciding if one identity service is worth twice as much as another during authentication. In the user interface, for both the end user and the administrator, the weights are represented by stars.



RATING IDENTITY PROVIDERS

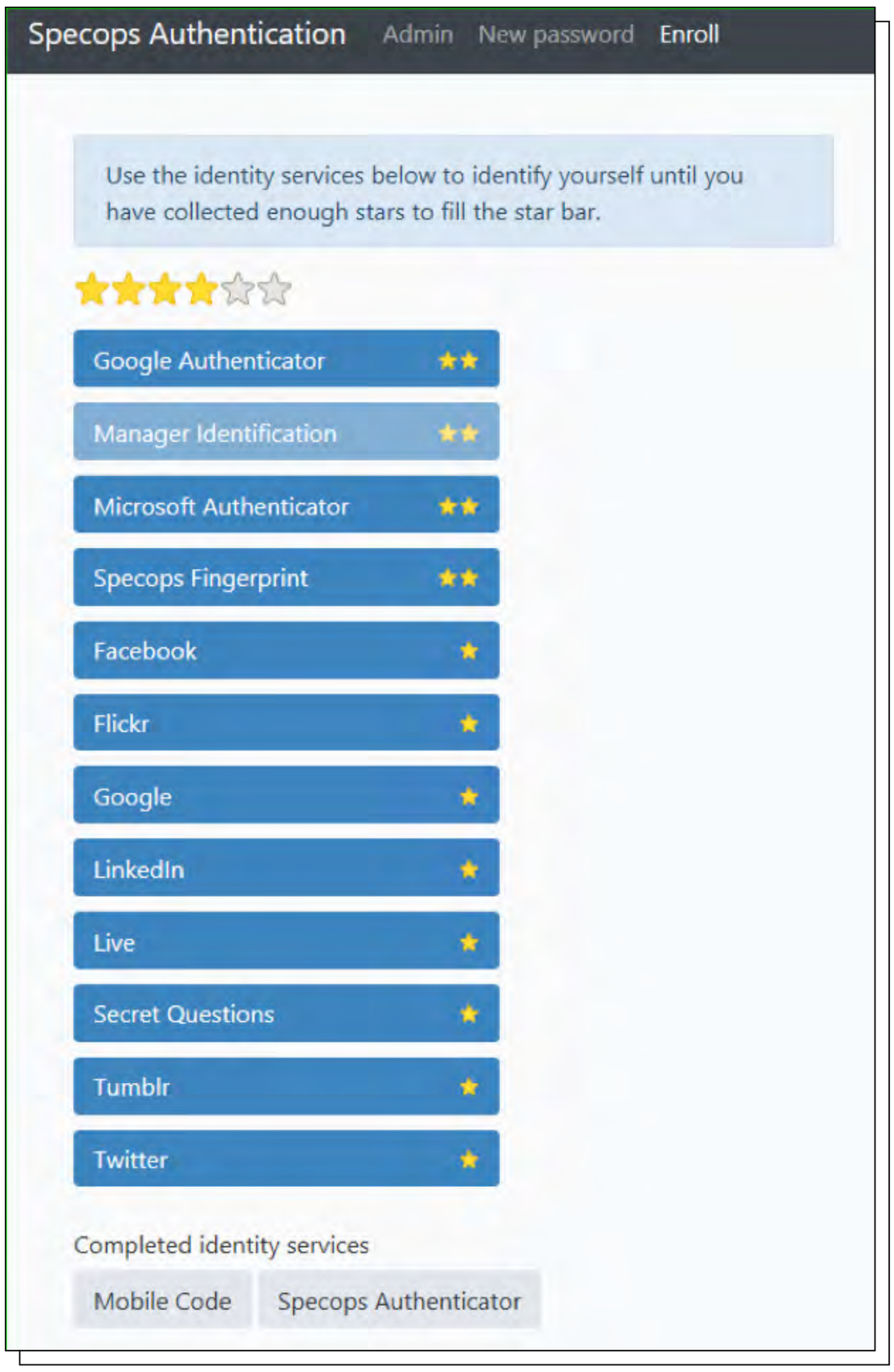
The user can choose the method or identity provider that is more convenient at a certain time. For example, if a user does not have a mobile phone at the moment of a password reset, it is possible to use a Microsoft Account or any other configured method for authentication.

Assigning a different value per Active Directory Group makes this feature even better and doesn't lower the bar in terms of security requirements. Users have different preferences during specific situations they might find themselves in, so this is a welcome approach for everyone: administrators, security officers and users.

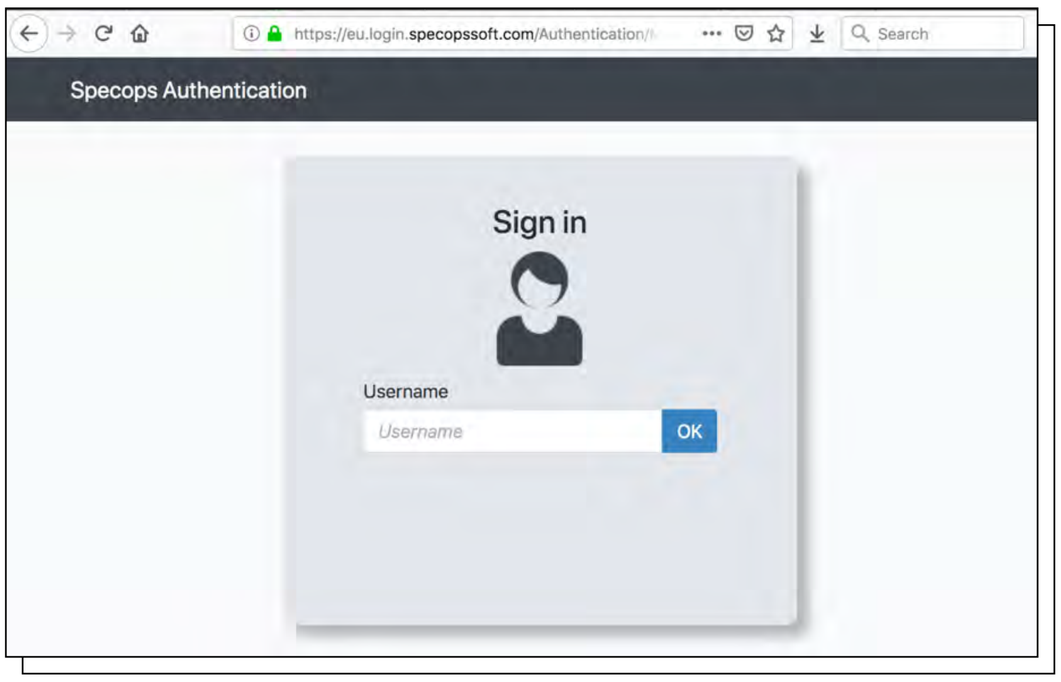
If your Active Directory is properly populated, users can be pre-enrolled for password resets using Specops uReset.

For most of the online services, users should and can enroll themselves to the online service they use. This consists of following a web link from the uReset user page and authentication with the target service.

To complete enrollment, the user has to collect enough stars to fill the star bar. Specops guarantees that activity on a given service is not monitored and data is only used for the password reset.



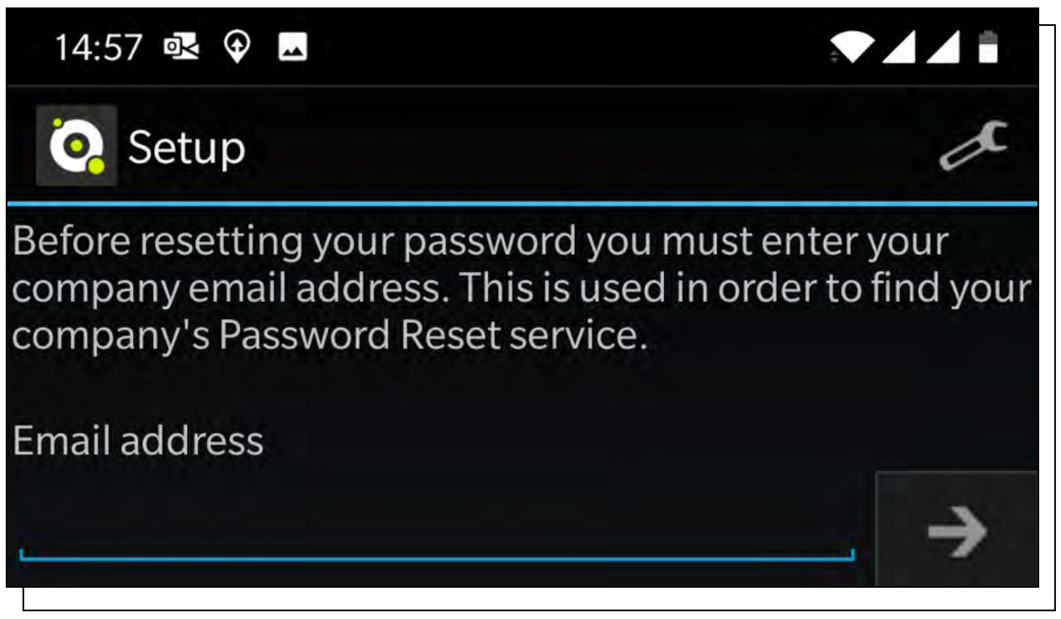
Once users are enrolled, they are ready to reset their password. To do that, they need to access the special link given in the configuration process with a web browser.



SPECOPS URESET LOGIN FOR USERS

When users reset their password, they will be able to see your password complexity requirements as they type in their new password. This prevents future frustration when a password change fails.

Another way to reset the password is through the mobile application. To use the mobile application, the user is required to enter an e-mail and, according to the given rules, the application will ask for specific identity verification (Mobile Code, social identity, etc).



SPECOPS URESET MOBILE APPLICATION LOGIN

Once everything is set up, the administrator doesn't have to spend any more time with this tool. Helpdesk workers will also appreciate this tool as they will not have to handle password reset requests on a daily basis.

Final thoughts

Specops uReset offers an innovative approach for password resetting:

- It provides users with the self-service option.
- It relies on multi-factor authentication and trusted third party authentication providers. What differentiates Specops from the competition is that they not only provide alternatives but also a weighing ability to ensure that security is not sacrificed e.g., the user does not have phone but can use Google and Facebook to authenticate.
- It allows organizations to decide which authentication factors they will use and which authentication providers they will trust.

The product works entirely as advertised. The installation process is simple and easy. The documentation provided is sufficient (although almost unneeded, as the interface is very intuitive).

If your helpdesk is spending too much time on resetting users' Active Directory passwords, you should try Specops uReset out.

2019

CLOUD SECURITY REPORT

Cybersecurity INSIDERS

UNCOVER

the Latest CLOUD SECURITY Trends

Organizations are continuing to adopt cloud computing at a rapid pace to increase efficiency, scalability and agility. 93% of them reported that they are moderately to extremely concerned about security in the cloud. Find out how organizations are planning to address their concerns in the **2019 Cloud Security Report**.

Download your copy of the (ISC)² sponsored report and learn:

- The latest cloud security trends and challenges
- How organizations are responding to security threats in the cloud
- What tools and best practices cybersecurity leaders are considering in their move to the cloud

Get the Report

Despite the many security drawbacks, the password continues to be an inexpensive authentication solution that works and is convenient in many scenarios.

True passwordless authentication is still quite a while away

AUTHOR_ Mirko Zorz, Editor in Chief, (IN)SECURE Magazine

The password has been one of the great inventions in the history of computing: a solution that allowed simple and effective identity and access management when the need arose for it.

Unfortunately, as time passed, the downsides of using (just) passwords became apparent: they can be forgotten, guessed, cracked, stolen and, finally, misused.

While we wait for the password to die...

During the last decade or so, many IT and IT security professionals have foretold the death of

the password, but that prophecy has yet to be fulfilled. Despite the many security drawbacks, the password continues to be an inexpensive authentication solution that works and is convenient in many scenarios.

But it's not the only authentication solution out there and, slowly but surely, the industry is taking steps toward a future without passwords.

> *To achieve a passwordless world, we need to solve the passwordless credential enrollment and account recovery puzzle.*

"The transition to truly passwordless authentication is going to be a journey," says Jim Ducharme, VP of Identity Products, RSA Security, and points out that, for the moment, all passwordless authentication is rooted and reliant on a password and username.

"While passwordless authentication is quite common on many devices (e.g., Touch ID and Face ID) accounts are still established with a password and if your device is lost or stolen, the account is recovered using a password," he notes.

To achieve a passwordless world, we need to solve the passwordless credential enrollment and account recovery puzzle, and to find a way for users to securely authenticate on devices that don't support biometrics and FIDO capabilities.

There's no one bulletproof solution

One of the things that are pushing enterprises to search for a suitable passwordless option is new data privacy regulation.

"Organizations are realizing that stolen identity is the number one security issue, and often the weakest link in security postures. With more at stake, including financial damages in the form of breach-related expenses, regulatory fines and the potentially irreparable loss of customer trust, we have already seen organizations start to adopt innovative and secure solutions to authenticate users seeking access to critical resources," he shared.

"Passwordless authentication reduces friction for the end user, eliminating complex, hard to remember passwords with another kind of credential like a hardware token, phone or biometric modality. Ultimately, it helps organizations better manage identity risks and protect what matters most."

But, he pointed out, no authentication solution is unhackable. And, while passwordless authentication can be more secure than the traditional password, like all forms of authentication it works best as one of several means of proving someone is who they claim to be.

"Authentication solutions should always be coupled with additional security layers to manage digital risk and a higher level of identity assurance," he advised.

Finally, it's also important to remember that a one-size fits all approach doesn't work for the varying identity and access managements needs across organizations and dynamic workforces.

> *While passwordless authentication can be more secure than the traditional password, like all forms of authentication it works best as one of several means of proving someone is who they claim to be.*

"As organizations continue to embrace digital transformation initiatives and consider regulations,

they must also continue to assess authentication needs and not place the burden of bulletproof security on one authentication solution," he warned.

Should you implement passwordless authentication across your large enterprise?

Before moving in that direction, CISOs must first pinpoint the organization's critical data and assets and think about how to best protect them.

"They must think through the entire credential lifecycle," Ducharme explained.

> *CISOs must look across the enterprise and consider the three dimensions of authentication (identity assurance, access assurance and activity assurance) and evaluate whether all can be achieved with passwordless authentication.*

This includes:

- Identity proofing (How do users obtain the passwordless credential? And what happens if they lose it?)
- What are the costs associated with supporting passwordless authentication?
- How does the new authentication method integrate with the enterprise's spectrum of applications? Including on-prem, infrastructure (Linux machines / network equipment), desktop, cloud and SaaS.
- Does the state of the organization's infrastructure support the technology and standards required to truly go passwordless?

CISOs must look across the enterprise and consider the three dimensions of authentication (identity assurance, access assurance and activity assurance) and evaluate whether all can be achieved with passwordless authentication.

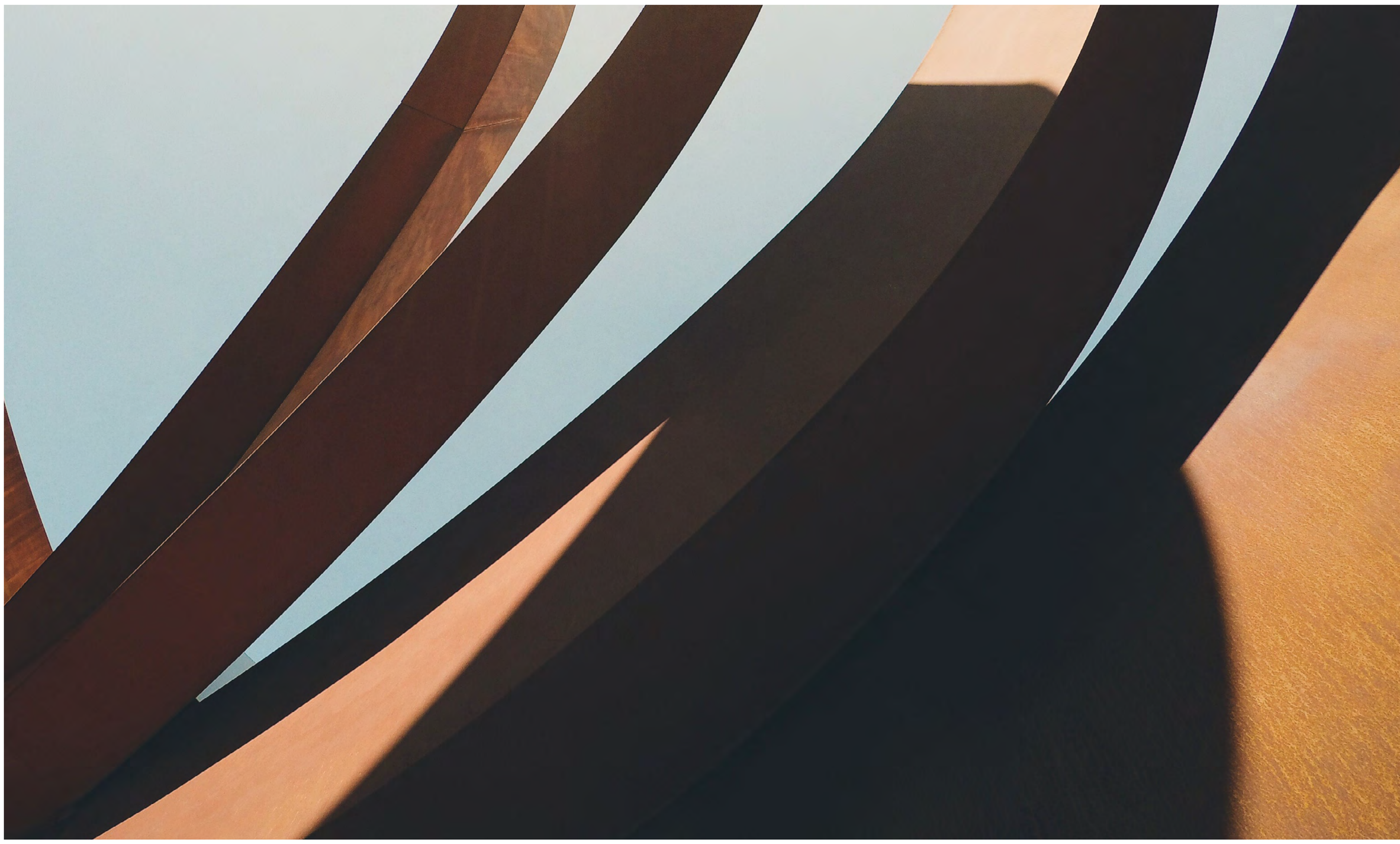
> *As we look at the cost of passwordless authentication, many people have a false sense that these new methods are much cheaper to implement because we are seeing password-less authentication experiences delivered for free in devices.*

"Identities are scattered everywhere, CISOs need a strategy that secures multiple points of access. Additionally, CISOs must keep the dynamic of the workforce and end users in mind – shifting the burden of secure authentication off users, reducing friction on the front end, and putting security control on the back end, where it belongs," he noted.
"To truly detect and manage identity risks, CISOs need to consider a risk-based authentication solution that is able to analyze user access, device, applications and behavior to provide businesses with the confidence that users are who they say they are based on previous history."

Finally, Ducharme warned that (front-end) passwordless authentication without the actual elimination of the underlying passwords (back-end) is not going to bring the savings associated with the reduction of password management, nor the security threats associated with passwords.

"As we look at the cost of passwordless authentication, many people have a false sense that these new methods are much cheaper to implement because we are seeing password-less authentication experiences delivered for free in devices," he said.

"However, there are still costs associated with organizations supporting these new devices, supporting the users leveraging these new features, as well as complexities associated BYOD environments."



Six criteria for choosing the right security orchestration vendor

AUTHOR_ Nimmy Reichenberg,
Chief Strategy Officer, Siemplify

Faced with the well-chronicled global skills shortage, the ceaseless bombardment of security alerts and the hodgepodge of security tools unable to communicate with each other, security operations professionals must feel as if the deck is stacked against them. But security orchestration, automation and response (SOAR) platforms have arrived on the scene to address the burgeoning problem of having too many disparate security tools firing off alerts without the adequate in-house talent to address them.

SOAR enables SecOps teams to integrate disconnected technologies and processes into a more cohesive security ecosystem.

SOAR enables SecOps teams to integrate disconnected technologies and processes into a more cohesive security ecosystem, allowing staff to

work more efficiently against the growing onslaught of cyber threats.

Look for a SOAR provider that not only supports many of the widely used security tools but also makes the integration of the tools quick and easy.

If you aren't already an adopter, you may be soon. Gartner predicts that "by year-end 2020, 30% of organizations with a security team larger than five people will leverage SOAR tools for orchestration and automation reasons, up from less than 5% today."

As a result, companies should exercise due diligence and have a clear criteria list when selecting a security orchestration vendor to ensure maximum value from their investment. While most providers have some unique features, there are several core functionalities you'll want to look for when choosing the optimal solutions for your needs.

1. Integration of disparate security solutions

The ability to integrate disparate security solutions is a basic characteristic of security orchestration, though not all SOAR solutions are created equal. As the SOAR market consolidates due to acquisitions, some SOAR products may lose their value if their available integrations become limited.

Vendor neutrality is key here. Look for a SOAR provider that not only supports many of the widely used security tools but also makes the integration of the tools quick and easy. In addition, consider a platform that allows you to create orchestrated and automated processes for these tools you have already invested in, from alerting and triage to investigation, remediation and collaboration. Here are some specific questions you should ask a prospective SOAR vendor:

- How many integrations do you support?
- Do you support both on-premises and cloud-based environments for those integrations?
- How quickly can you add or build new integrations?
- Will we be able to create/customize our own integrations?

2. Automated processes with playbooks

The right technologies are crucial to the success of security operations teams, but their effectiveness is only as good as the processes in place for using them. A key ingredient to any successful SecOps program is having a good set of playbooks that help security analysts create consistent, repeatable and automated response processes for accomplishing tasks and determining tools that come into play if a threat alert is raised. For example, the process for malware alerts is different than one for phishing alerts or data exfiltration.

While the basis behind playbooks is to allow for the automation of various use cases, their functionality should be used for more than just putting tools into automated processes. Try to partner with a vendor that provides a breadth of features for playbook creation and customization.

Hunt for a vendor with an interface that minimizes the amount of switching required and that pushes the most critical cases to the top so your team can improve its focus and prioritize bringing down response and resolution times.

Questions to ask:

- Do you include standard playbooks to help get our team started?
- Can your playbooks be customized to meet

our organization's needs and desired levels of automation?
- How easy will it be for our team to create new playbooks?
- Does your platform support tests and simulations to ensure playbook effectiveness?

Hunt for a vendor with an interface that minimizes the amount of switching required and that pushes the most critical cases to the top.

3. Visual investigations

While some alerts and cases can be fully automated and then closed, most require human analysis. To understand a threat, security analysts normally draw out key pieces of information from the huge pile of raw data they've manually collected from alerts, logs, threat intelligence and other sources. These analysts then lay the pieces out to obtain an overview of the situation, build a storyline and perhaps discover relationships among events.

While this investigation technique is effective in visualizing a threat storyline, the common practice relies heavily on manual and time-consuming methods, such as laying things out on a whiteboard. Look for a security orchestration vendor whose solution mirrors an analyst's visual investigation process: reinforced with graphs, timelines, flows and representations of relevant entities, which can significantly speed up investigation and response times.

Questions to ask:

- What is your solution's visual investigation capabilities?
- Does the solution just run the playbook and hope the analyst figures things out or does it also provide insights and guide the analyst toward solving the puzzle?
- How would our analysts build the timeline of a security event?
- How are relationships among entities (IPs, users files, etc.) represented?
- What level of detail is provided about each entity and how?

4. The SOC workbench

Console switching is unavoidable in security operations, especially because analysts typically run multiple tools and handle different cases at the same time. Depending on the moment, one screen might be isolating hosts, while another screen might be blacklisting executables, with a third screen focusing on correlation and trending, and so on. Having to switch from console to console while prioritizing cases is not only time consuming, but also confusing.

Hunt for a vendor with an interface that minimizes the amount of switching required and that pushes the most critical cases to the top so your team can improve its focus and prioritize bringing down response and resolution times.

Your SOAR vendor should be able to help you understand how your SOC is performing. From there, you can make informed decisions about everything from processes and tooling to caseloads and staffing.

Questions to ask:

- What is the breadth of activity our team can manage through the interface?
- How does the platform prioritize and assign cases?
- How difficult is it to understand the user interface? Is there a certain skill level required or can our analysts become expert users quickly?

- Are there any collaboration capabilities included in the platform?

5. Case management and alert grouping

While advanced log aggregation tools and security information and event management solutions (SIEMs) can help bring together the data you need in one place, you still may be challenged to extract the true positives and weed out the false negatives. Plus, on any given day, a security operations center might be besieged by hundreds or even thousands of alerts. If each alert becomes its own case to be worked by an analyst, think about the management impact and collaboration required to effectively handle them. Analysts working cases containing multiple related alerts can manage, triage and close these as a single effort. At the very least, alerts need to be correlated using threat intelligence and other data sources to understand what's really happening before being able to proceed with incident response and remediation.

Because different stakeholders will want to look at different metrics and KPIs depending on their role, your chosen solution should be able to provide the information they require without burdening your security analysts.

Questions to ask:

- Does your platform group related alerts into manageable cases?
- How do you determine if alerts are related or not?
- How are cases created from alerts?
- Does the solution use machine learning for alert prioritization and analyst assignment?

6. Reporting

Your SOAR vendor should be able to help you understand how your SOC is performing. From there, you can make informed decisions about everything from processes and tooling to caseloads and staffing. Because different stakeholders will want to look at different metrics and KPIs depending on their role, your chosen solution should be able to provide the information they require without burdening your security analysts.

Questions to ask:

- Do you support turnkey and automated reporting?
- What are your dashboarding capabilities? Do they offer templates or the ability to customize?
- Can we schedule reports to automatically run and be distributed on a set schedule?

Security orchestration solutions can elevate a SOC's capabilities, efficiency and effectiveness. However, careful examination in selecting your ultimate partner can maximize the value of your investment.

In summary, look for a vendor that will streamline your security operations, reduce missed and uninvestigated alerts, speed up response, enable the creation of consistent and predictable processes, allow better transparency of metrics, and increase your SOCs ability to improve over time.

BIGGEST EVER HITB EVENT RETURNS TO THE UNITED ARAB EMIRATES

HITB+CyberWeek: a gathering of the world's leading thinkers and cyber security subject matter experts in the UAE.

Driven2Pwn

Prize money of **USD 1.5 million** in an all-new coordinated bounty contest!

AI Competition

USD 100,000 up for grabs if your AI can run pentests and evade malware.

Cyber Battle of the Emirates

A CTF for the **best and brightest students**.

PRO CTF

The world's top 25 CTF teams competing for **USD 100,000**!

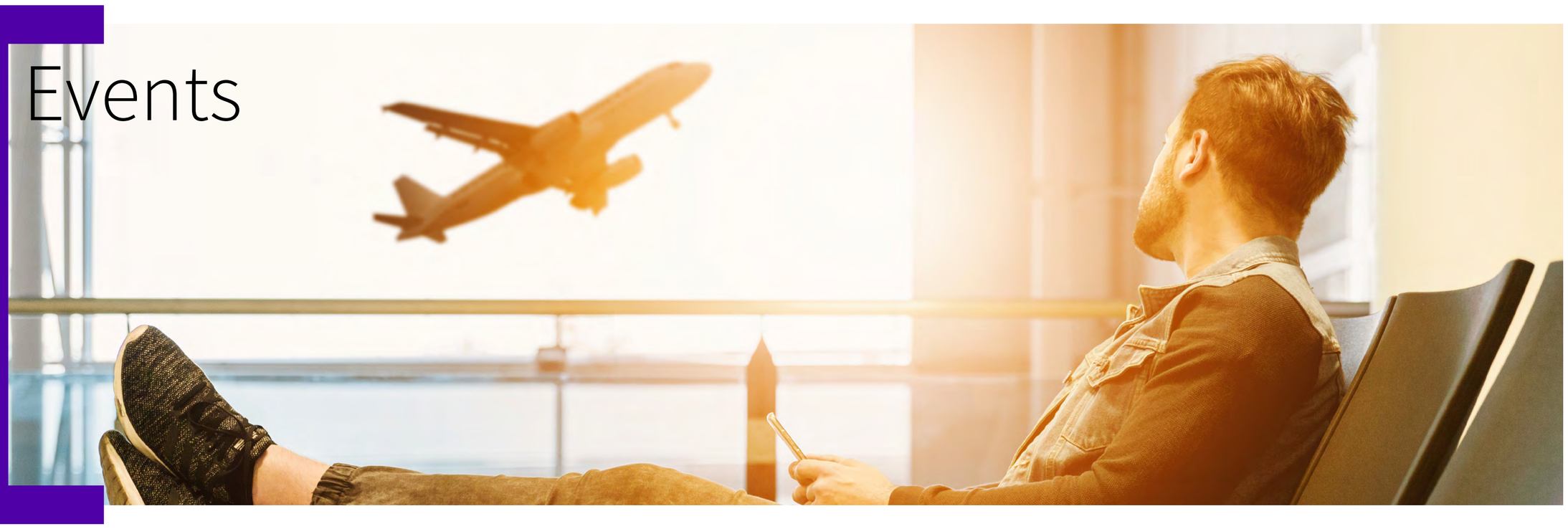
HITB+CyberWeek

Abu Dhabi, UAE: 12-17 October 2019

Emirates Palace,
Abu Dhabi, United Arab Emirates

12 - 17 October 2019
https://cyberweek.ae

Events



(ISC)2 Security Congress 2019

October 28-30, 2019
Walt Disney World Swan and Dolphin Resort, Orlando, FL, USA
http://congress.isc2.org/d/pbqql6?RefID=helpnet

(ISC)2's 2019 Security Congress will unite industry colleagues from around the globe for three days of education, best-practice sharing and networking in a variety of formats.

With more than 100 tactical, focused learning opportunities, this event will advance a global perspective and vision as our premier conference for cybersecurity professionals.

With hands-on learning opportunities like CISSP, CCSP, Security Architecture and CISO 2-day training courses, Career Center, and a Networking Night at House of Blues, this is the conference to add to your must-attend list. (ISC)2 members are eligible for special discounted pricing and will earn CPEs.

HITB+CyberWeek

October 12-17, 2019
Abu Dhabi, UAE
https://cyberweek.ae

Hack In The Box (HITB), known for its cutting-edge technical talks and trainings in computer security, is launching its biggest global event to be held in Abu Dhabi, UAE from 12-17 October 2019. HITB+CyberWeek will bring together the world's top thinkers and cyber security experts to share their latest knowledge, ideas and techniques among security professionals but also students.

HITB+CyberWeek will feature:

- World's top 25 Capture the Flag teams competing in a new style of attack and defense contest featuring a record-breaking prize pool of US$100,000
- The best bug hunters and ethical hackers competing in an all-new coordinated bug bounty contest with US$1.5 million to be won
- New challenge for Artificial Intelligence (AI) enthusiasts with US$100,000 in prize money to develop future cyber security tools using machine learning
- Growing knowledge and nurturing capabilities with a Capture the Flag competition for high school and university students, bringing the winners of Belgium and Germany's Cyber Security Challenge to Abu Dhabi for the finals

Ensuring supply chain security: 5 IT strategies for choosing vendors wisely

AUTHOR_ Randy Barr, CISO, Topia

With the proliferation of SaaS solutions, API integrations and cloud computing, virtually everything in the modern enterprise is connected to an untold number of outside entities. In fact, many business processes depend on this connectivity, even when doing so broadens the threat landscape and puts the organization at greater risk.

Most often, the problem arises because IT is brought into the vendor evaluation process after a selection has already been made.

This interconnectedness means that vendor vulnerabilities become your vulnerabilities. For proof, we need look no further than the massive NotPetya attack that took down hundreds of companies in the summer of 2017. What began as a quasi-cyberwarfare attack on the Ukraine crippled everything from global shipping giant Maersk to

a hospital in Pennsylvania, causing $10 billion in losses—all essentially collateral damage. The incident brought the risk of vendor security front and center as the ransomware spread like wildfire, even to organizations that had absolutely no connection to the original targets.

> *Ensuring that as many security and compliance boxes as possible are checked prior to IT review keeps IT from having to pull the plug on deals at the last minute.*

When it comes to implementing better supply chain cybersecurity risk management, little has changes since then. A recent Gartner study found that 83% of organizations uncover third-party risks after conducting due diligence, and over 70% of business and IT executives admit to having no idea how diligent their third-party partners are when it comes to security. Disturbingly, over half say they rely on trust alone.

With so much at stake, it's extremely troubling that so many organizations fail to make supply chain security a top priority. Most often, the problem arises because IT is brought into the vendor evaluation process *after* a selection has already been made. Business units are empowered to conduct initial assessments and due diligence and bring the vendor for IT/security review only once the contract is ready to be signed. That means the IT department becomes the "bad guy" when they pump the brakes or bring the deal to a halt.

To overcome this problem, IT must take a more strategic approach to ensuring supply chain security by equipping business units to evaluate vendor security earlier in the process.

Here's how to prepare business units to vet suppliers more thoroughly during due diligence and keep IT from having to step in at the last minute to nix the deal.

1_Train everyone on cybersecurity risks. Working in IT, you live, eat, breathe and sleep cybersecurity. But other employees likely do not. They're not hyper-aware of the relentless risks and most would be shocked if they knew realized the width of the threat landscape organizations face. That's why training is critically important. Make cybersecurity training a routine requirement so that those making vendor decisions—and even just everyday users—understand where the risks lie and how to mitigate them. By raising awareness, you build a more vigilant front-line defense.

2_Establish a baseline security policy. Create a set of specific guidelines, policies and controls requirements that vendors must meet in order to pass muster. This should include things like security training for internal staff, two-factor authentication, secure development policies, lifecycle management, penetration testing, asset management, mobile device security, change and access controls, and even physical/environmental requirements. By putting your vendor requirements in writing and making them non-negotiable, business units can conduct more thorough due diligence before presenting the vendor for security review.

3_Demand compliance verification. Make sure business units understand the critical importance of compliance with any mandates that govern your business or industry. In today's environment, you are responsible for both your own and your vendors' compliance. That means, in the event of a vendor breach, your company could be held equally responsible in some cases. Insist on proper documentation of compliance with GDPR, PCI, HIPAA, etc. And, remember, different markets have different requirements, so make sure business units know their vendors must show proof of compliance with mandates in the regions or countries in which you do—or will do—business.

4_Ask to see the data flow. At a basic level, most companies rely on cloud resources for storage or computing—virtually no one operates their own in-house datacenter. That means your data, connected to their systems via API, travels outside their network and is potentially exposed to numerous other vendors, contractors and other third parties with whom they do business. You have a right—and a responsibility—to know what that data flow looks like and who is potentially in contact with your data. Business units should ask to see a data flow diagram. If the vendor claims that is proprietary information, they should consider that a red flag.

5_Adopt a continuous, iterative approach to vendor security. Too many organizations rely on moment-in-time verification of protocols or certifications, but today's business environment and threat landscape change far too quickly for an annual audit. Gartner suggests an iterative approach to reduce risk at the speed of modern business by identifying and remediating third-party risks before they have an impact. Making vendor compliance review an iterative process doubles your capacity to remediate risks, saving your organization a tremendous amount of time, money and frustration.

Giving business units a playbook for vendor security screening prior to (or as part of) contract negotiation arms them with the knowledge and capability to conduct more thorough due diligence. Ensuring that as many security and compliance boxes as possible are checked prior to IT review keeps IT from having to pull the plug on deals at the last minute. This not only protects the organization, but also eliminates the adversarial relationship between IT and the rest of the business, replacing it with a more cooperative, collaborative one.

zscaler™

Secure your cloud transformation

Trusted by hundreds of the Forbes Global 2000 organizations to provide:

A fast user experience
for internet and Office 365

Security stack delivered as a service
identical protection for all users, all locations

Secure SD-WAN
optimizes MPLS costs; no appliances

Seamless remote access
no VPNs, no hassles

Learn more at zscaler.com

Connectivity is a key aspect of daily life and the connected services often revolve around mobile devices. There's an app for pretty much anything you want to do and mobile apps can be a vital part of the economics of a business.

To ensure they can play such an important role, a business' mobile apps will often contain critical information. Also, in a software-defined world, a lot of IP can be wrapped up in them. All this makes them a very attractive target for hackers.

It's no longer enough to focus just on network or perimeter security and no longer safe to assume that new software and devices aren't constantly changing the risks to the system.

Have you thought about the often-overlooked mobile app threat?

AUTHOR_ Catherine Chambers, Senior Product Manager, Irdeto

The real problem organizations face in today's connected world is that the traditional approach

to software security is no longer adequate. It's no longer enough to focus just on network or perimeter security and no longer safe to assume that new software and devices aren't constantly changing the risks to the system. Instead, organizations must employ a defense-in-depth strategy that factors in the evolving nature of security and cybercrime trends.

Organizations in many sectors never expected connectivity to apply to them in such an all-encompassing way. As a result, they are fighting an ongoing battle to evolve their security thinking and strategies in tandem with the increasing threat vector, as mobile devices and apps proliferate across their businesses.

Accepting hostility

Organizations must accept that mobile devices are a hostile environment and that application security has a big part to play in protecting mobile apps in such an environment.

Irdeto recently polled 700 security decision makers in global enterprises and found that only 52% of companies are currently using mobile app protection as a security measure. This could be partly because security is often an after-thought in the development of mobile apps, and difficult to integrate properly later on. It could also be due to the fact that many companies still rely on standard mobile security measures such as Mobile Device Management (MDM)/Mobile Application Management (MAM), app wrapping and authentication.

But although these measures are valuable, security needs to be more extensive, particularly if there is critical IP in the app.

One recent example of the impact that a hacked business app can have can be gleaned from an incident involving a well-known maker of farming machinery. The organization attempted to roll out a service application that mandated that all equipment maintenance must be performed by authorized technicians, but the lack of software security led to application licenses being easily circumvented. As a result, both the anticipated service revenue and the direct application revenue was dramatically curtailed.

With this in mind, when you deploy sensitive mobile apps in any environment you will have to implement a sound application protection strategy and have the right tools in place.

There are three crucial elements which organizations must consider when it comes to AppSec.

The first is to **design security in**. Unfortunately, in today's rush to get to the minimum viable product stage as quickly as possible, security is usually considered less important than design and development. On top of that, plenty of software developers are not familiar with secure software development and do not have a standard set of best practices to work with. They need security training at the beginning of the software development lifecycle. Also, a security design review should be done by a reputable application protection vendor or threat and risk assessment specialist.

Secondly, organizations must **apply layered software protection techniques to their apps and APIs.** Mobile apps can be reverse engineered, repackaged and redistributed, their functionality can be tampered with, they can have malware injected into them, IP can be lifted from them, or they can simply be copied/cloned. Apps with critical data require strong, multi-layered software security, which should include data security at rest and in transit, network/API security and robust

software protection for IP. The apps can also be protected by code hardening tools to conceal proprietary algorithms and secrets, including cryptographic keys, private and personal data and credentials.

Finally, organizations must **develop a monitoring, maintenance and feedback plan,** as application security should never be "set and forget". It requires ongoing monitoring (detection), maintenance (renewal) and feedback (assess or reassess) – best practices that are embodied in common Secure Software Development Lifecycles to ensure effective adaptation to new threats. Software protection tools should offer easy diversification and renewability to generate an entirely new instance of secured code with a simple change of a random seed.

The right security strategy needs the right skills

While it's clear that organizations' security strategies need to evolve to meet the ever-changing security challenges faced by today's connected businesses, many industries are not prepared to tackle the problem. This isn't to say that organizations aren't doing their part to implement cybersecurity technology and strategies. However, the integration of a wide range of devices that may or may not be secure, coupled with evolving regulations and requirements to address cybersecurity challenges, has created an extremely confusing security landscape that's difficult to navigate.

The key to implementing the right security strategy is having the right skills, and this is where organizations in many industries face additional challenges, as the skills required can often be in short supply. For example, the 2017 Global Information Security Workforce Study by the Center for Cyber Safety and Education found that Europe will have a cybersecurity skills workforce gap of 1.8 million by 2022. In addition, a report the same year from Cybersecurity Ventures estimated that there will be 3.5 million unfilled cybersecurity jobs globally by 2021, up from one million in 2016.

Research from Irdeto and Vanson Bourne earlier this year found that only 7% of organizations across the globe have everything they need to tackle cybersecurity. Further, 46% stated that their organization needs additional expertise/skills within the organization to address all aspects of cybersecurity and more than one-third (34%) need more staff to help manage cybersecurity.

While this is potentially a societal challenge that extends from the number of people training in cybersecurity at university right into the workplace, this doesn't help organizations struggling with the increased cybersecurity threat brought about by connectivity. To overcome the skills challenge, organizations need to find automated ways of applying security that works. For example, machine learning can provide the intelligent component to decide where and how security should be applied and offer automated app protection.

> *The bottom line is that to combat the increasing vulnerabilities, all companies participating in the ecosystem must be on top of their game. If you want to take advantage of the benefits of connected devices or software, you need to choose wisely where to spend your time and budget.*

However, many automated solutions on the market still typically require cybersecurity expertise to configure, build and apply proper protection, which is not of help to organizations that are struggling with a cybersecurity skills shortage. Proper app security needs to be easy to apply

in the future. It must use machine learning to provide organizations with assurance that apps are provided with expert-level protection against hackers and cyberthreats, without the need for the app developer to know anything about security or to implement any security code.

> *The sad truth that organizations must accept is that cybercrime is a business where hackers have the advantage.*

Building a secure future

The benefits of connectivity brought to a wide range of industries are not in doubt, but greater connectivity opens organizations and their customers up to a myriad of additional vulnerabilities that must be considered from the outset. The sad truth that organizations must accept is that cybercrime is a business where hackers have the advantage. In addition, deploying mobile apps in a hostile environment where they can be easily reverse engineered or copied puts the business and potentially its customers at risk. It leaves the door open to theft of IP, theft of service revenue and may create a possible gateway into your enterprise through unauthorized use of the app.

However, it's not all gloom and doom for connected industries. According to Irdeto's research, of the security decision makers surveyed, 99% agreed that a security solution should be an enabler of new business models, not just a cost. These findings suggest that organizations are thinking even more strategically about security and give a clear indication that today's businesses realize the value add that security can bring to their organization. From enabling new rental or subscription models in connected vehicles, to Digital Twins revolutionizing the manufacturing processes, to providing patients with even better healthcare, security is the enabler to successfully implementing new and future business models in today's connected world.

The bottom line is that to combat the increasing vulnerabilities, all companies participating in the ecosystem must be on top of their game. If you want to take advantage of the benefits of connected devices or software, you need to choose wisely where to spend your time and budget. Whatever the nature of the threat, organizations must understand the scope of their current risk, ask hard cyber-centric security questions to vendors, and work with trusted security partners to cover any knowledge gaps and safely embrace connectivity in their business.

Know Your Adversaries

Be Cybersecurity Enlightened

We help your organization become cybersecurity enlightened. With Anomali you can detect threats, understand adversaries, and respond effectively.

Learn more: www.anomali.com