[+] (IN)SECUREMagazine

03 | 2019
ISSUE 61.5

#RSAC 2019

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

RSA Conference, the world's leading information security conferences and expositions, concluded its 28th annual event in San Francisco.

The week saw more than over 42,500 attendees, 740 speakers and 700 exhibitors at Moscone Center and Marriott Marquis, where they experienced the North and South Expo, keynote presentations, peer-to-peer sessions, track sessions, tutorials, seminars and special events on topics such as privacy, hackers and threats, machine learning, artificial intelligence and the human element, law, IoT security, public interest technology, and talent shortages.

"At RSA Conference, we strive to showcase unique content from the world's top cybersecurity minds, and the latest security solutions, in a way that connects us all, reveals diverse perspectives, and creates a safe space for tackling the tough issues we all face," said Linda Gray Martin, Director & Chief of Operations of RSA Conference. "We are proud of our attendees, exhibitors, and speakers that made this goal a reality over the past week. We thank everyone involved for bringing their passion and commitment to improving cybersecurity, and our world, to RSA Conference year after year."

Platinum sponsors of our coverage from RSA Conference 2019

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

Photography by RSA Conference and (IN)SECURE Magazine.

Cybersecurity skills gap worsens, security teams are understaffed

As emerging technology and threat landscapes experience rapid transformation, the skillsets need to change as well.

80 percent of 336 IT security professionals Dimensional Research polled on behalf of Tripwire believe it's becoming more difficult to find skilled cybersecurity professionals, and nearly all respondents (93 percent) say the skills required to be a great security professional have changed over the past few years.

The survey found that while 85 percent report their security teams are already understaffed, only 1 percent believe they can manage all of their organization's cybersecurity needs when facing a shortage of skilled workers. Nearly all respondents (96 percent) say they are either currently facing difficulty in staffing security teams due to the skills gap or can see it coming.

Of those, 68 percent are concerned with losing the ability to stay on top of vulnerabilities, 60 percent worry about being able to identify and respond to issues in a timely manner and stay on top of emerging threats, and 53 percent fear they will lose their ability to manage and secure configurations properly.

In addition, respondents were also asked if they would benefit from outside security help.

Sale of SSL/TLS certificates on the dark web is rampant

There is no dearth of compromised, fake and forged SSL/TLS certificates for sale on dark web markets, researchers have found.

Web Name	SSL Certificates	TLS Certificates	Ransomware	Zero-Day Exploits
Dream Market	2912	64	512	160
Wall Street Market	10	4	13	1
BlockBooth	3	1	0	0
Nightmare Market	2	0	5	0
Galaxy3	16	7	1	0

TLS certificates are sold individually and packaged with a wide range of crimeware. Together these services deliver machine-identities-as-a-service to cybercriminals who wish to spoof websites, eavesdrop on encrypted traffic, perform man-in-the-middle attacks and steal sensitive data.

The researchers dove into online markets and hacker forums that were active on the Tor network, I2P and the Freenet from October 2018 to January 2019 and searched for "for sale" ads of compromised, fake and forged TLS certificates. They conducted 16 weekly searches, discovering nearly 60 relevant online markets webpage on Tor and 17 webpages on I2P, and reviewed the listings in detail and, in some cases, engaged in conversation with sellers to gain a better understanding of the goods and services being sold.

Key study findings include:

- Five of the Tor network markets observed, offer a steady supply of SSL/TLS certificates, along with a range of related services and products.
- Prices for certificates vary from $260 to $1,600, depending on the type of certificate offered and the scope of additional services.
- Researchers found extended validation certificates packaged with services to support malicious websites such as Google-indexed "aged" domains, after-sale support, web design services, and integration with a range of payment processors – including Stripe, PayPal and Square.
- At least one vendor on BlockBooth promises to issue certificates from reputable Certificate Authorities along with forged company documentation – including DUNS numbers. This package of products and services allows attackers to credibly present themselves as a trusted US or UK company for less than $2,000.

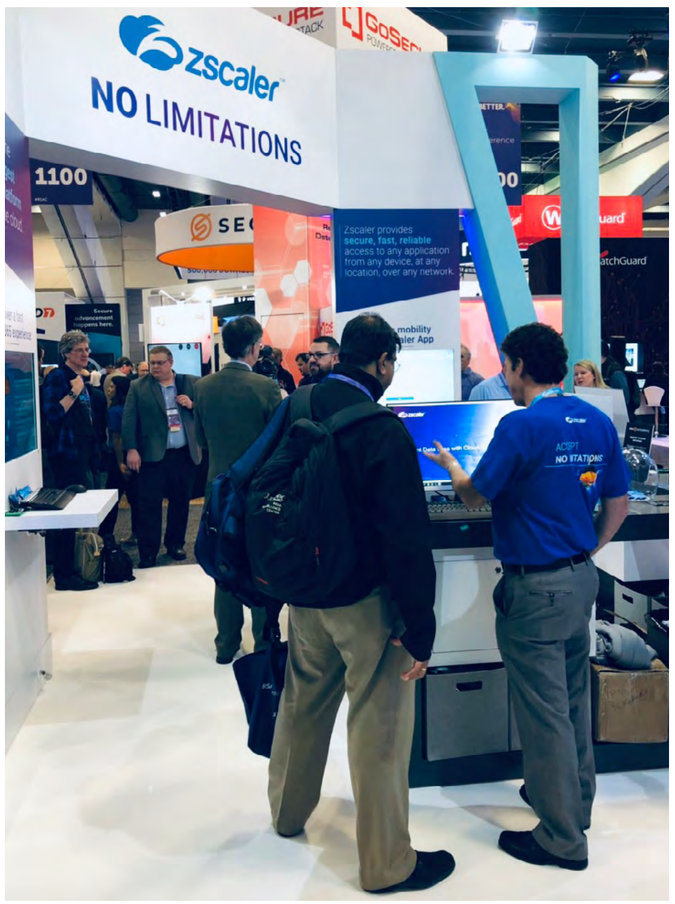
Fidelis Cybersecurity offer Threat Research as a Service

Fidelis Cybersecurity, a leading provider of threat detection, threat hunting, and response solutions, announced the launch of Threat Research as a Service (TRaaS), a subscription-based offering which provides access to the Fidelis Threat Research Team of experts for tailored threat intelligence and countermeasures.

As part of the new subscription-based model, Fidelis will provide, at client request, Fidelis Intelligence Services, Malware Services, and/or Threat Research Consulting Services for malware analysis and reversing, intelligence briefs, and threat hunting engagements and workshops.

Subscribing to Fidelis TRaaS will provide customers with the capability of in-depth research and analysis to produce intelligence reporting, analyze or reverse engineer malware samples, and produce countermeasures necessary to detect and stop adversary attacks and exploitation.

#RSAC 2019 gallery



The patterns of elite DevSecOps practices

The 6th annual DevSecOps Community Survey of 5,558 IT professionals conducted by Sonatype in partnership with CloudBees, Carnegie Mellon's Software Engineering Institute, Signal Sciences, 9th Bit, and Twistlock, revealed that organizations with elite DevSecOps programs are outperforming other enterprises by extreme margins. Those factors include:

DevOps automation – Elite DevSecOps practices are 350% more likely to have fully integrated and automated security practices across the DevOps pipeline. They also have increased feedback loops that enable security issues to be identified directly from tools.

Open source controls – 62% of respondents with elite programs have an open source governance policy in place where automation improves adhere to it, compared to just 25% of those without DevOps practices.

Container controls – 51% of respondents with elite practices say they leverage automated security products to identify vulnerabilities in containers, while only 16% of those without said the same thing.

Training – Organizations with elite DevSecOps practices are 3x more likely to provide application security training to developers than those organizations without DevOps practices.

Preparedness – 81% of those with elite practices have a cybersecurity response plan in place compared to 62% of those without DevOps practices.

Capsule8 expands leadership team with key executive hires

Capsule8, the only company providing high-performance attack protection for Linux production environments, announced additions to its executive team, appointing Jim Bandanza as Chief Operating Officer/CRO and Kelly Shortridge as Vice President of Product Strategy.

The announcement was made at RSA Conference 2019, where Capsule8 was a finalist in the RSAC Innovation Sandbox Contest. The company earned the finalist designation for its unique approach to protecting Linux production workloads at massive scale, whether containerized, virtualized or bare metal.

As Capsule8's Chief Operating Officer/CRO, Jim oversees all aspects of the company's global field operations. He has more than 25 years of executive management experience at leading and advising cloud and cybersecurity companies including running all field activities for RSA for several years. Kelly brings expertise in innovative defensive research, threat modeling and market analysis to Capsule8. Kelly's role at Capsule8 driving product strategy follows successful tenures at SecurityScorecard, BAE Systems Applied Intelligence, IperLane and Teneo Capital.

Basil Security unveils security policy enforcement solution

Basil Security announced the world's first policy-as-code platform that provides stateful security policy enforcement over arbitrary code execution, APIs, and data access. Basil can be used to prevent errors, block insider cyberattacks, and guarantee accountability.

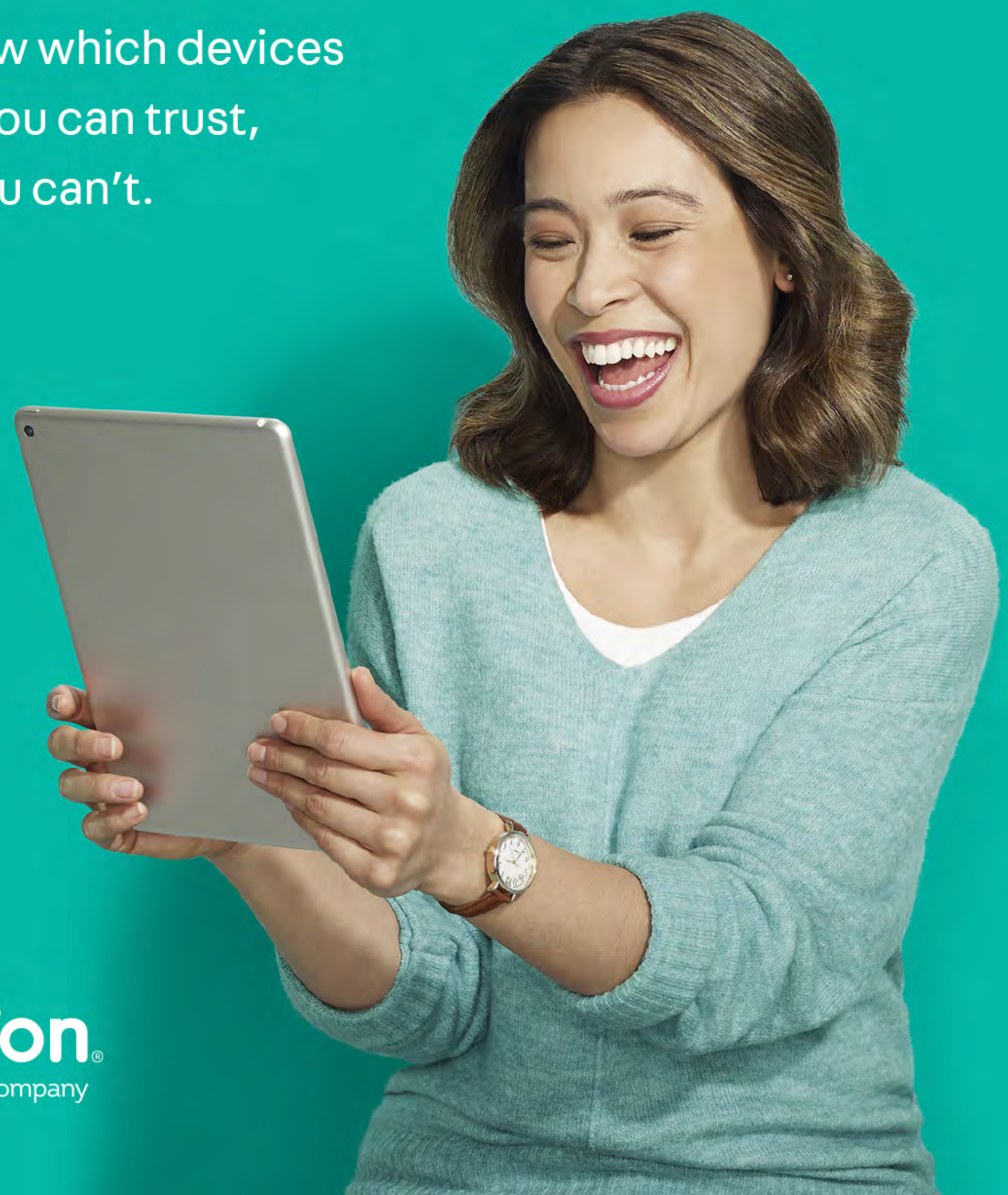
Basil integrates with and extends existing IAM capabilities with next-generation attribute-based access control (ABAC). Using Basil, human-readable security policies are proactively enforced. Basil can control arbitrary code execution, APIs, and data access, and adds multi-party approval, non-repudiation, immutable, unified audit logging, and other new capabilities.

Basil operates at the infrastructure, platform, and application levels across all cloud-based environments. It is ideal for security and regulatory audits, digital forensic investigations and attribution, and DevSecOps—including development and operations (DevOps), and continuous integration and delivery (CI/CD).

Together with ABAC, immutable, unified audit logging provides selective visibility to internal and external auditors, as well as to end users, including the ability to audit prior points in time.

We make it safer for you to do business online.

Instantly know which devices and people you can trust, and which you can't.



iovation®
A TransUnion® Company

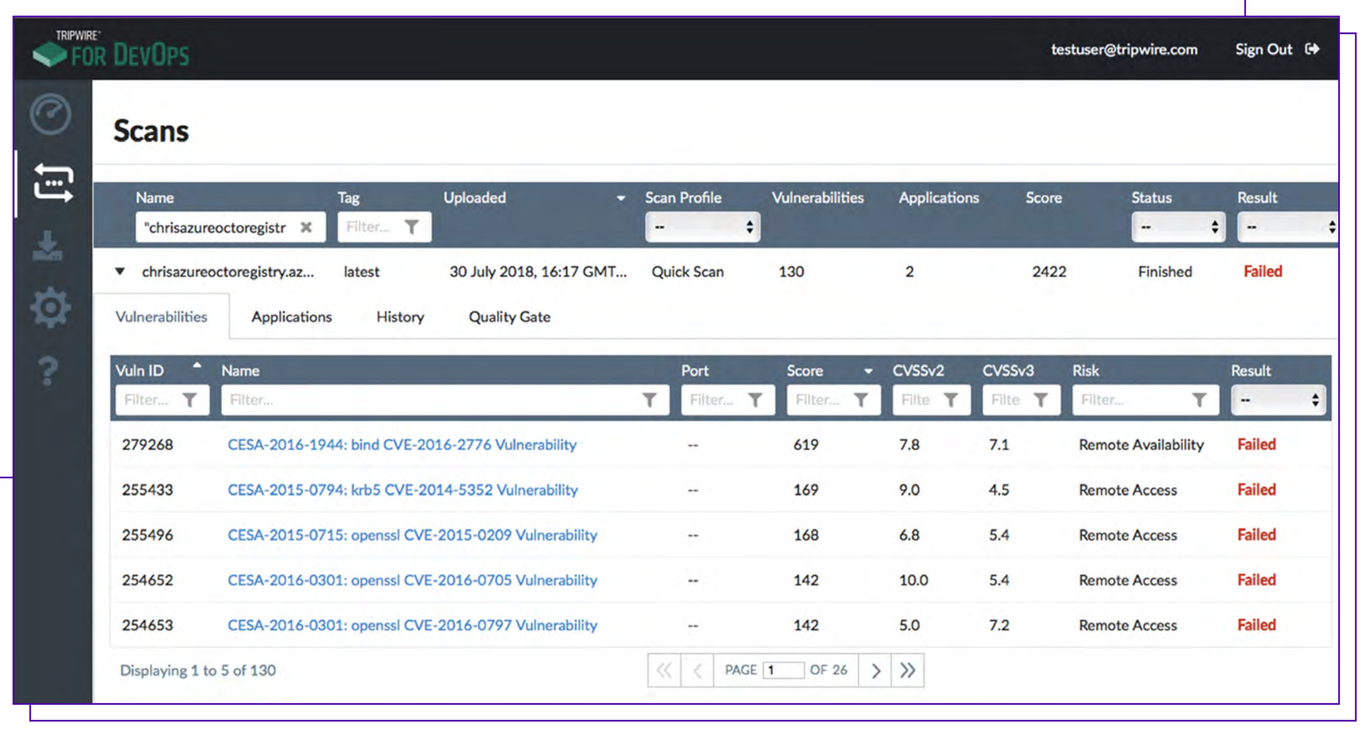
Tripwire expands coverage and support for DevOps environments

Tripwire announced Tripwire for DevOps, a software-as-a-service (SaaS) solution that provides configuration assessment and vulnerability management in containers across the DevOps life cycle.

By fully automating the assessment of container images in the continuous integration/continuous deployment (CI/CD) pipeline and dynamically testing live instances of application containers in an isolated, cloud-based sandbox, Tripwire for DevOps can establish quality gates at each stage that ensure defined security standards are met. It can also be used to simply monitor and assess repositories, providing visibility into potential risks and without interference to the process.

Tripwire for DevOps has expanded its support to include:

- Google Container Registry
- Quay.io remote registry
- Docker Registry HTTP API V2
- Amazon Elastic Container Registry (ECR)
- Windows and Linux AMIs



SentinelOne turns every protected endpoint into a network detection device

SentinelOne unveiled SentinelOne Ranger – turning every protected endpoint into a network detection device capable of identifying and controlling every IoT and connected device on a network.

SentinelOne Ranger gives machines the ability to detect and protect other machines, enabling them to become environmentally aware and fend off attacks from one another, without human intervention. Using AI to monitor and control access to every IoT device, SentinelOne allows machines to solve a problem that has been previously impossible to address at scale.

The technology can not only fingerprint and profile devices the SentinelOne agent discovers from enabling complete environment visibility, but can also identify if any aspect of that environment is dangerous. It is the industry's first solution that allows machines to autonomously protect and notify security teams of vulnerabilities, rogue devices, and anomalous behavior.

Cyberbit launches SCADAShield Mobile for passive monitoring of ICS network traffic

Cyberbit announced the official launch of SCADAShield Mobile, a portable unit for monitoring and auditing Industrial Control System (ICS) networks.

Housed in a 27-pound, water resistant suitcase small enough to stow in the cabin of an airplane, SCADAShield Mobile enables on-demand audits and provides asset discovery, threat detection and vulnerability assessment for use cases ranging from on-site compliance audits to understanding the security posture of an ICS network during an emergency.

SCADAShield Mobile is designed for first responders, service providers, auditors and critical infrastructure network managers to passively monitor ICS network traffic. Using the same Deep Packet Inspection technology that powers Cyberbit's industry-leading SCADAShield enterprise solution, SCADAShield Mobile works by plugging into the SPAN port of a network switch.

Within hours it creates a comprehensive map of the Operational Technology (OT) network, a detailed asset inventory report and a list of vulnerabilities, potential threats, and misconfigurations.

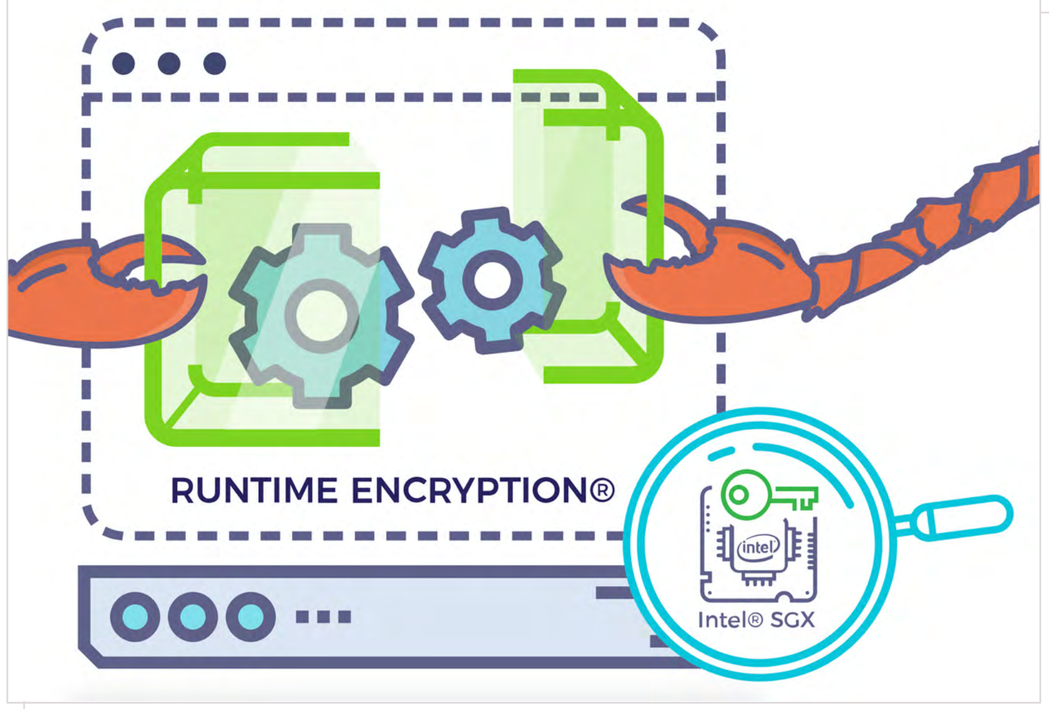
Criminal groups promising salaries averaging $360,000 per year to accomplices

New research from Digital Shadows reveals that criminal groups are promising salaries averaging the equivalent of $360,000 per year to accomplices who can help them target high-worth individuals, such as company executives, lawyers and doctors with extortion scams.

These salary promises can be higher still for those with network management, penetration testing and programming skills – with one threat actor willing to pay the equivalent of $768,000 per year, with add-ons and a final salary after the second year of $1,080,000 per year.

One principal method of extortion where criminals deem potential victims to be particularly vulnerable is so-called ‘sextortion’. Researchers tracked a sample of sextortion campaigns and found that from July 2018 to February 2019 over 89,000 unique recipients faced some 792,000 extortion attempts against them. An analysis of Bitcoin wallets associated with these scams found that sextortionists could be reaping an average of $540 per victim.

Extortion is in part being fuelled by the amount of ready-made extortion material readily available on criminal forums. These are lowering the barriers to entry for wannabe criminals with sensitive corporate documents, intellectual property, and extortion manuals being sold on by more experienced criminals to service aspiring extortionists. Blackmail guides, for example, are on sale for less than $10.



Fortanix launches Rust-based SDK for Intel SGX applications

Fortanix launched its Enclave Development Platform (EDP), which provides a native Rust-based SDK to write Intel Software Guard Extensions (Intel SGX) enclaves.

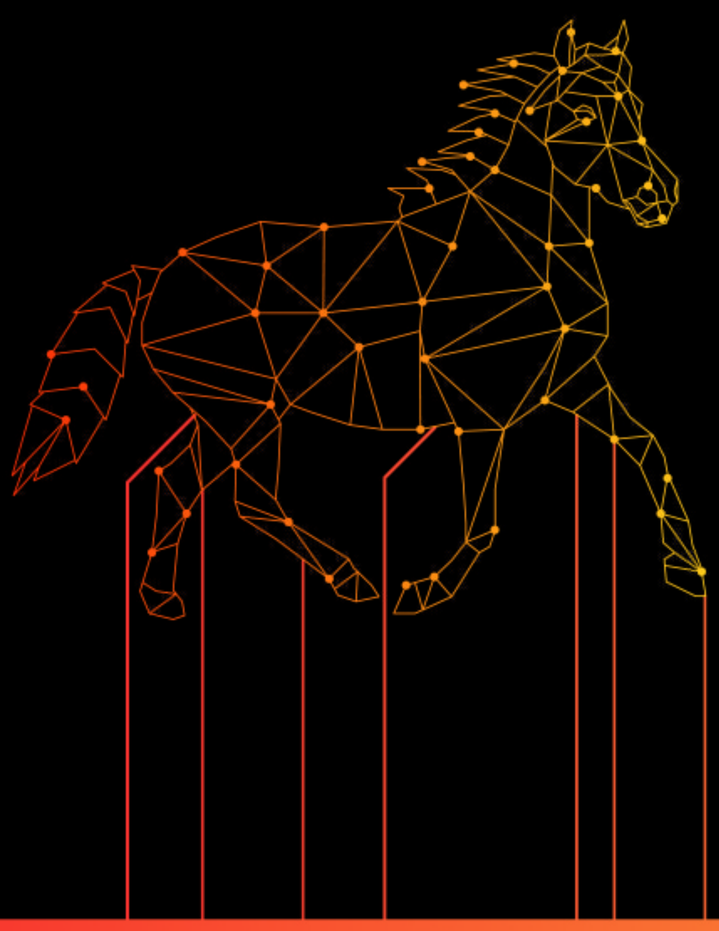
The Fortanix EDP is an open source SDK that uses the state-of-the-art security properties of the Rust language and Intel SGX to deliver a more secure application development platform.

The Fortanix EDP is fully integrated with the Rust compiler, which allows developers to immediately use new features including non-lexical lifetimes, futures and async/await syntax, and improved compile-time speeds. Due to Rust’s stability, old code will continue to work after the compiler is upgraded.

The open source licensing of the Fortanix EDP allows developers to build and sell or distribute the applications they create.

VISIBILITY

RELIABILITY



PROTECTION

ALL NODES LEAD TO TRIPWIRE

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Our award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management.

Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

tripwire®

Axonius named most innovative startup at RSA Conference 2019

RSA Conference announced that Axonius was selected winner of the fourteenth-annual RSAC Innovation Sandbox Contest.

Duality Technologies was recognized as well by the judges for building SecurePlus platform for secure collaboration on sensitive data.

In its fourteenth year, the RSAC Innovation Sandbox Contest is a leading platform for startups to showcase their groundbreaking technologies that have the potential to transform the cybersecurity industry. Past winners include companies such as Phantom, Invincea, UnifyID and, most recently, BigID.

Axonius is a cybersecurity asset management platform providing actionable visibility and policy enforcement for all assets and users.

"I am blown away that the judges recognized a problem as mundane as asset management to be the winner this year," said Nathan Burke, chief marketing officer of Axonius. "It is amazing that a really big and nagging problem that hasn't been solved yet is something that the judges decided is worthy of winning."

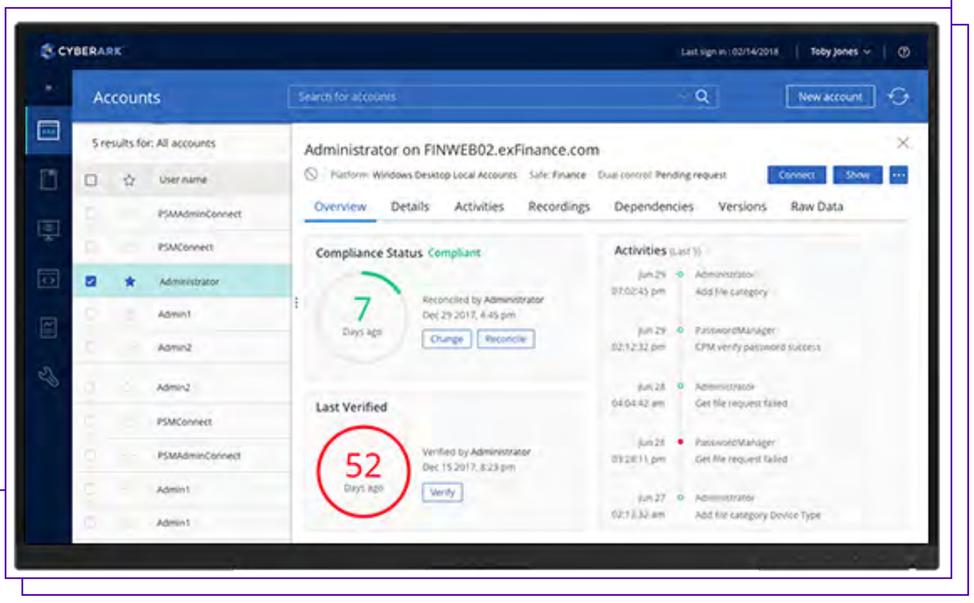
CyberArk simplifies privileged access security in cloud environments

CyberArk announced ground-breaking new capabilities to simplify the continuous discovery and protection of privileged accounts in cloud environments.

The CyberArk Privileged Access Security Solution v10.8 is the first-of-its-kind to automate detection, alerting and response for unmanaged and potentially-risky Amazon Web Services (AWS) accounts. This version also features new industry-leading Just-in-Time capabilities that deliver flexible user access to cloud-based or on-premises Windows systems.

With the new v10.8 release, the CyberArk Privileged Access Security Solution sets a new standard by delivering the industry's most comprehensive approach to security and operational efficiency in the cloud through:

- Continuous privileged account discovery
- Automated privileged exploit detection and response
- Simplified deployment in AWS environments
- Just-in-Time access with flexible provisioning options.



RSA extends SIEM capabilities with expanded analytics, threat aware authentication

RSA unveiled the newest version of the RSA NetWitness Platform, which features machine learning models based on deep endpoint observations to rapidly detect anomalies in user's behavior to uncover evolving threats.

New capabilities in RSA NetWitness Platform 11.3 include:

Threat-aware authentication with RSA SecurID Access: RSA NetWitness Platform now fuels threat-aware authentication to enable continuous authentication and the ability to block insider threats and malicious actors in the act of an attack while reducing the time and effort by overworked security operations teams.

RSA NetWitness UEBA: RSA NetWitness Platform introduces the first machine learning models based on deep endpoint process data collected by RSA's Endpoint Detection and Response (EDR) Solution, RSA NetWitness Endpoint. This advanced analytics capability can rapidly detect anomalies in user's behavior and uncover unknown, abnormal, and complex evolving threats that may be otherwise missed by analyzing logs alone.

RSA NetWitness Endpoint 11.3: The only fully native endpoint detection and response solution within an evolved SIEM, to equip security analysts with industry-leading detection, investigation, and incident response capabilities.

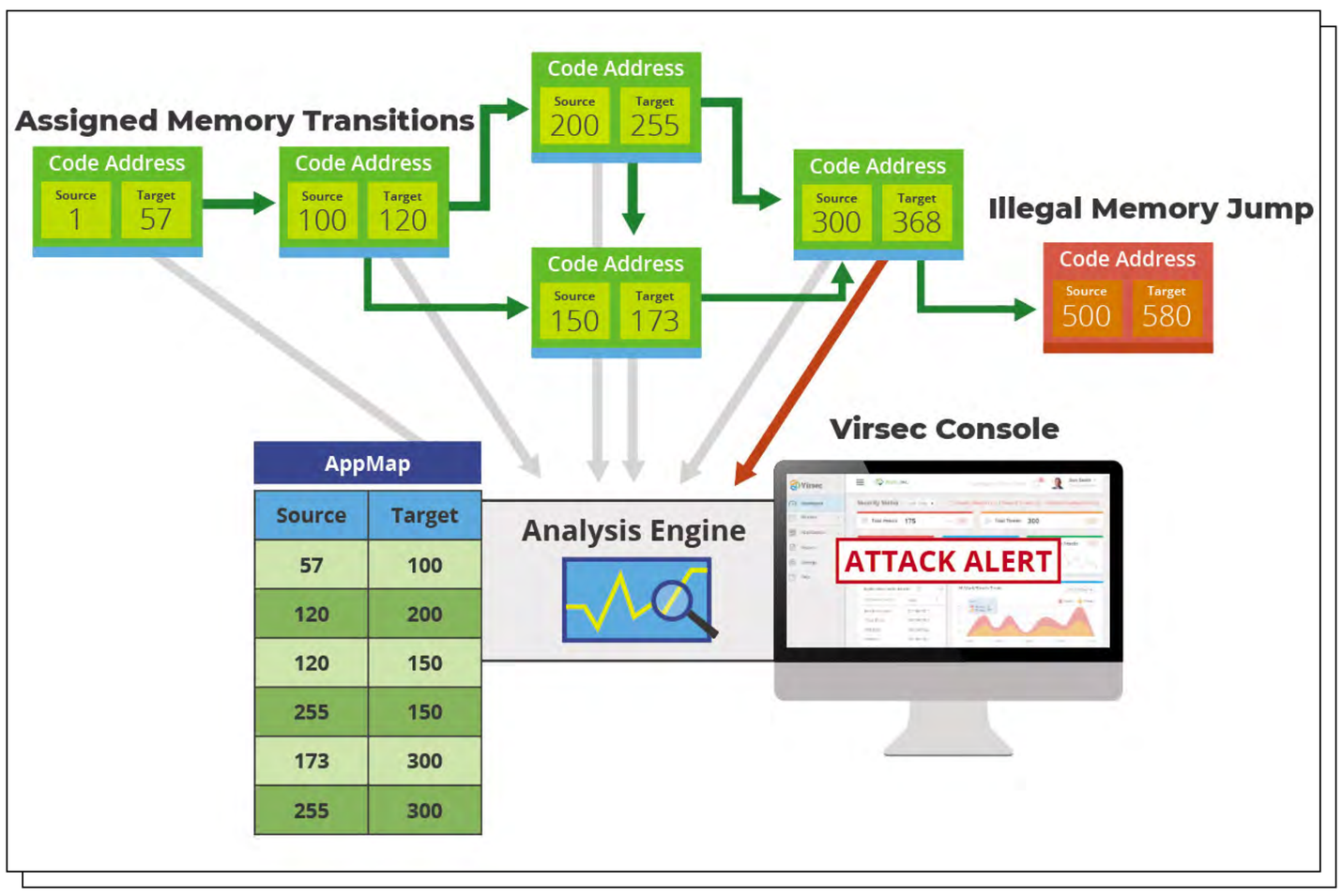
Key 2019 cybersecurity industry trends

Momentum Cyber revealed six key cybersecurity trends that it predicts will drive M&A and IPO activity in the cybersecurity industry in 2019:

- Identity and Access Management (IAM) will continue its strong performance as perimeters continue to fade and we adopt more of a zero-trust approach to security
- Hybrid cloud computing utilization will continue its rise and drive demand for cloud-agnostic solutions to address security, data protection, and compliance
- Data centric security solutions will continue their rise as data discovery, management, and protection extends security beyond today's evaporating perimeters
- IoT devices will continue to be targeted given their low level of security and exponential growth into our homes, cars, medical devices, IT networks, OT networks and critical infrastructure
- A volatile stock market and expanding buyer universe will make later stage companies view M&A as an even more attractive alternative to an IPO, further increasing M&A deal volume
- Security services providers will continue to increase market share as more organizations elect to use managed solutions to alleviate vendor fatigue and the growing cybersecurity skills shortage.

Virsec debuts application memory firewall to stop fileless attacks

Virsec launched its new Application Memory Firewall, which delivers a comprehensive set of memory protection capabilities that secure the critical juncture between applications and process memory.



This advanced memory protection solution is the first product to detect deviations in application execution caused by memory-based attacks and take immediate action to stop applications from being corrupted or hijacked, without requiring code changes, patches or signature updates.

Virsec effectively detects and stops advanced fileless and zero-day techniques including buffer overflow attacks, stack smashing, DLL injections, return-oriented programming (ROP) and ROP gadgets, side channel attacks and corruption of configuration data.

Virsec's patented technology automatically maps the legitimate execution of an application. If there is any deviation during execution, this is a positive sign of compromise, and the Application Memory Firewall stops the exploit within microseconds.

Radiflow releases new version of its industrial threat detection solution

In the new version (v5.3.) of its iSID industrial threat detection solution, Radiflow has added a dedicated risk analytics module that automates vulnerability mapping and assessment processes. This new risk analytics module dynamically evaluates vulnerabilities according to the classification of attacker profiles and defense strategies for protecting specific functionalities and operational processes.

Based on the attacker models and defined defense strategies, iSID dynamically calculates a risk and exploitability score for each device on the OT network and the most critical attack vectors using these scores.

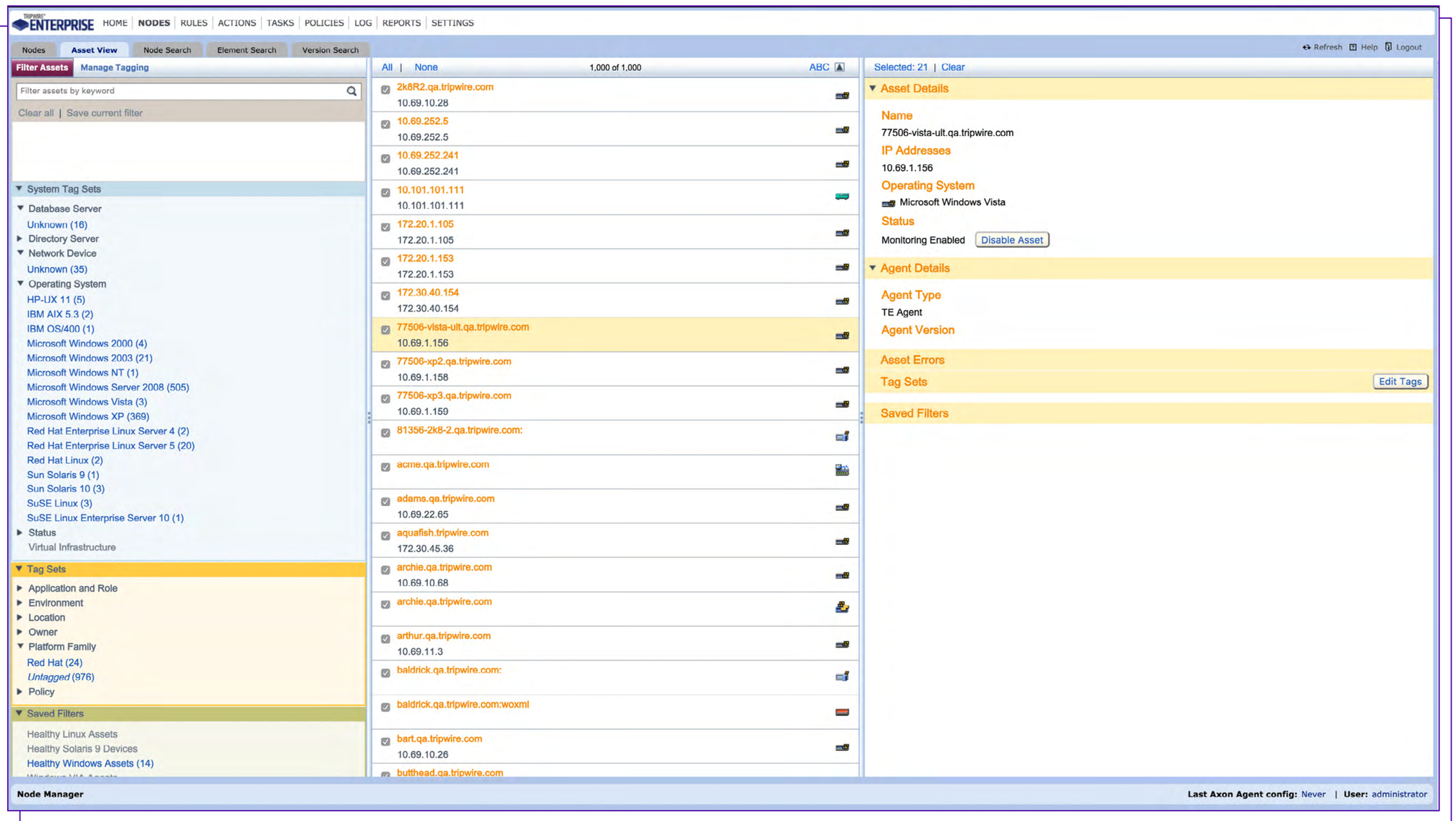
These scoring and mapping capabilities add important value to the cybersecurity efforts of industrial enterprises as security analysts and risk managers can prioritize workloads to remedy vulnerabilities based on the specific context of their OT networks and impact on the business operations of the organization.

FROM TICKETS TO TURBINES

DigiCert delivers the uncommon denominator in TLS/SSL, IoT and PKI solutions. From creating the industry's most-advanced, hyperconverged infrastructure, to designing certificates for the post-quantum age, we're committed to finding a better way to secure what comes next.

digicert.com/uncommon

digicert®
THE UNCOMMON DENOMINATOR



Tripwire launches vulnerability management as a service

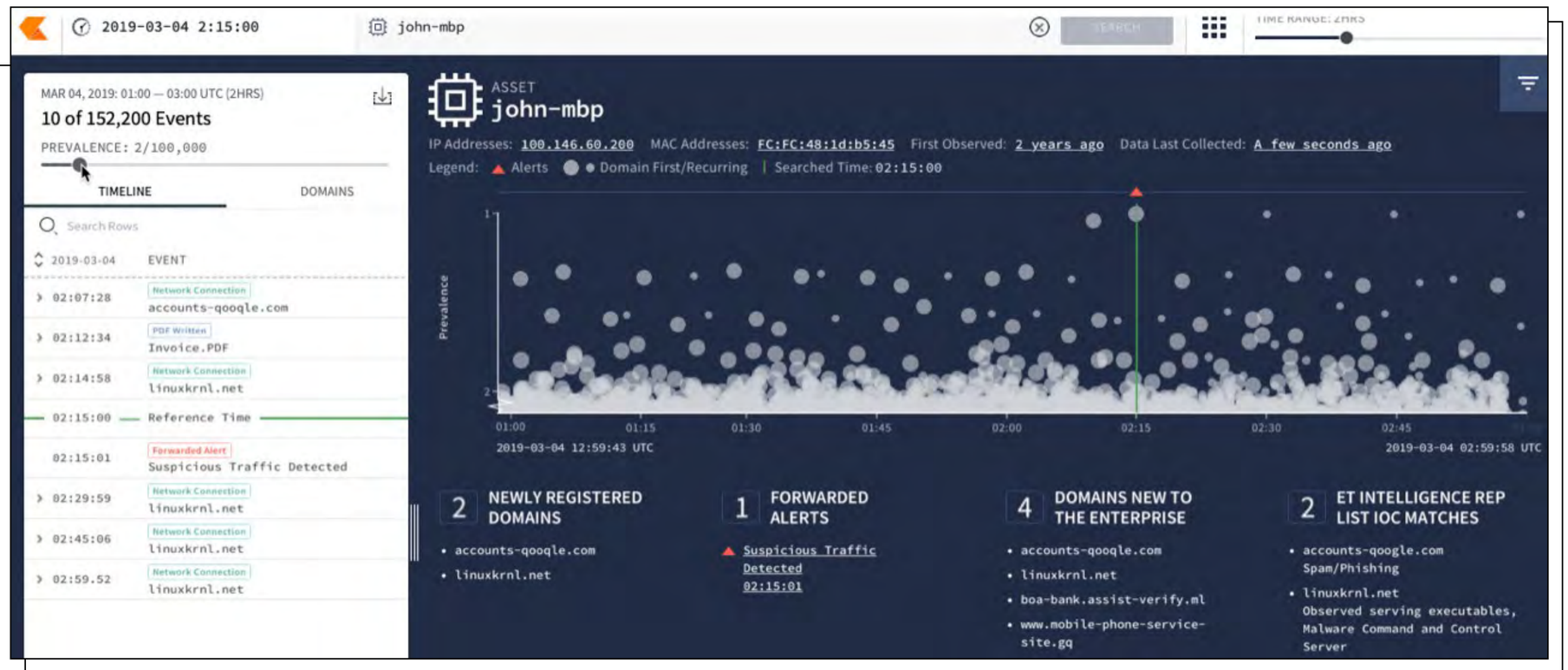
Tripwire announced the expansion of Tripwire ExpertOps to include vulnerability management as a managed service.

With this addition, organizations with limited in-house cybersecurity resources can take advantage of the Tripwire ExpertOps service to maintain a strong foundation of security, from vulnerability management (VM) to security configuration management (SCM) and file integrity monitoring (FIM).

Tripwire ExpertOps reduces the workload and complexity of managing critical security controls through personalized consulting and managed services. The new ExpertOps VM capabilities leverage the industry-leading capabilities of Tripwire IP360, the company's enterprise-class vulnerability management solution. Tripwire's VM capabilities offer a comprehensive view of vulnerability risks along with actionable reporting and recommendations.

Tripwire's vulnerability management is backed by comprehensive coverage of more than 200,000 conditions (including vulnerabilities, configurations, applications and operating systems) and timely vulnerability intelligence through the Tripwire Vulnerability and Exposure Research Team (VERT).

Tripwire ExpertOps provides personalized consulting from trained experts and hands-on tool management for compliance and critical asset security. It augments in-house security teams with ongoing support, guidance and customized reporting, and provides insights when security incidents occur. The services also include executive-level reports indicating status toward security goals and objectives and insight into areas of improvement.



Chronicle creates Backstory, a cloud service for analyzing enterprises' security data

Chronicle, the cybersecurity subsidiary of Alphabet (Google's parent company), has announced Backstory, a cloud platform that can be used by enterprises to sift through their historic security data: DNS traffic, netflow, endpoint logs, proxy logs, and so on.

Backstory is a global cloud service where companies can privately upload, store, and analyze their internal security telemetry to detect and investigate potential cyber threats.

It Backstory normalizes, indexes, and correlates the data, against itself and against third party and curated threat signals, to provide instant analysis and context regarding risky activity.

The service is meant for companies that generate massive amounts of security telemetry and have trouble hiring trained analysts to make sense of it.

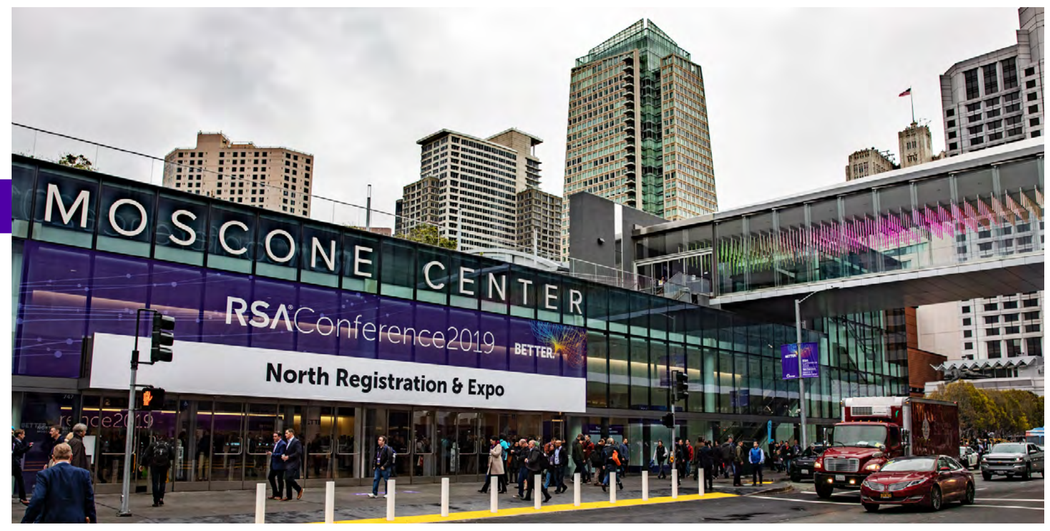
Adaptiva automates remediation of endpoint compliance, security issues

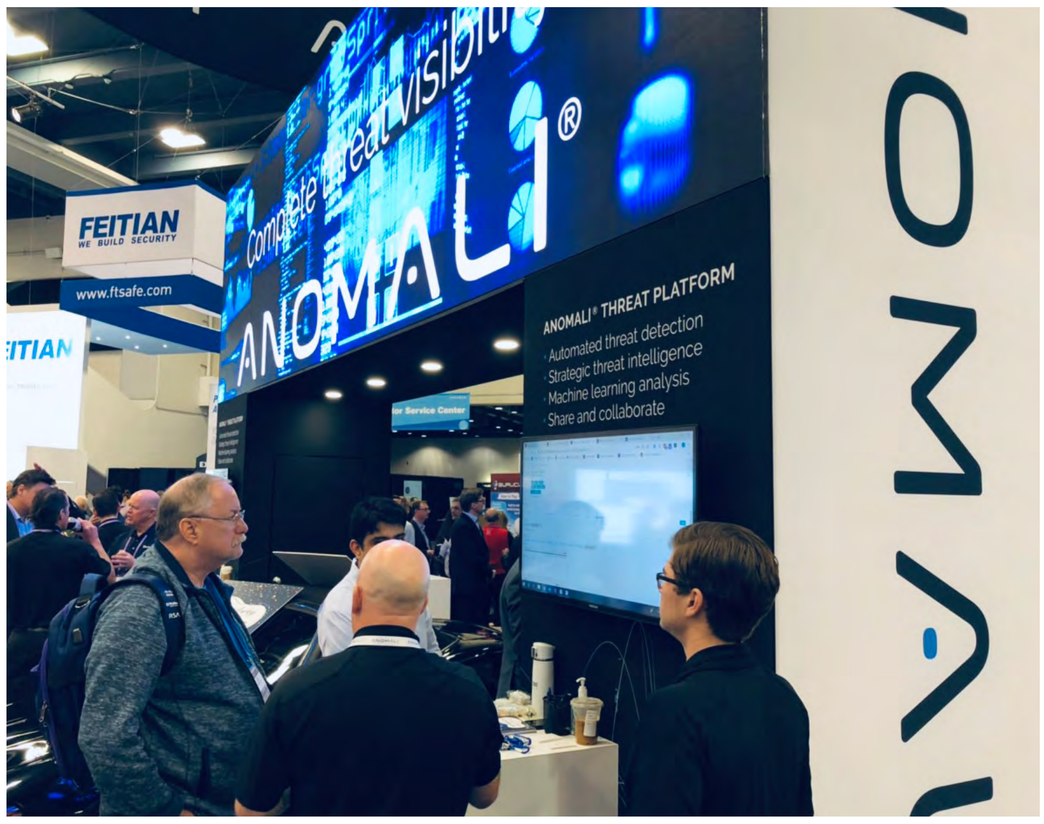
Adaptiva, a global provider of endpoint management and security solutions for enterprise customers, launched a new endpoint compliance and vulnerability management product, Evolve VM.

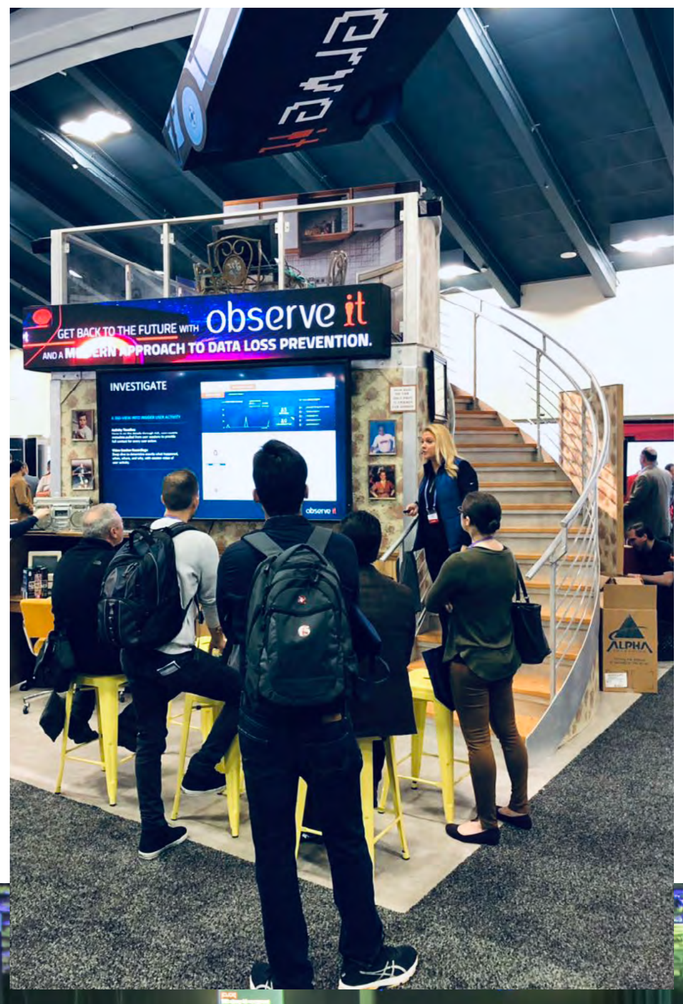
Evolve VM leverages Adaptiva's industry-leading, intelligent peer-to-peer platform to automatically check for thousands of compliance issues and security vulnerabilities across an enterprise's endpoints, diagnose any problems, and instantly fix those issues without requiring network resources or impacting the end users.

It eliminates the need for intensive manual efforts while protecting the network.

#RSAC 2019 gallery







Armor Scientific makes authentication as easy as walking into a room

Armor Scientific released the Armor Platform, a converged hardware token and middleware suite aimed at law enforcement, first responders, government, military, finance, healthcare and transportation.

A combination of wearable GPS, biometric hardware, and patent-pending cryptographic and blockchain-enabled middleware, the Armor Platform removes the complexity around identity governance, making authentication as easy as walking into a room.

It authenticates and authorizes users without the need for a username, password or any other personal information, enables every user and device to be added as a node to an assurance domain powered by cryptographic keys and a blockchain ledger, and protects access and only allows activity once the consensus of multiple other nodes have been reached.

Growing mobile cybersecurity incidents spur plans for increased security investment

A majority of RSA attendees plan to spend more on mobile security in the coming year, Lookout has discovered.

Since critical data has moved to the cloud, employees are able to access it from any network, wherever they are in the world. In fact, 76 percent of the 100 polled RSA Conference attendees access corporate data from personal mobile devices and/or public WiFi networks.

Key findings from the survey include:

Growing mobile cybersecurity incidents
— 1 in 10 pollees report that their organization has experienced a mobile cybersecurity incident or breach in the past 12 months

Increasing mobile security investment
— 52 percent of pollees plan to increase their mobile security spend in the next 12 months, underscoring a growing awareness of mobile security risk.

Mobile security habits
— 76 percent of pollees have accessed their corporate network, corporate email or corporate cloud services from a personally-owned mobile device or tablet. Additionally, 76 percent of them have accessed their corporate network, corporate email or corporate cloud services from a public WiFi network, such as a coffee shop, airport or hotel.

Focus on securing connections to corporate email, messaging apps and storage
— Most commonly, RSA attendees reported using their mobile devices to access corporate email (85%), messaging, such as Slack (53%), and storage services, such as Google Drive or Box (43%).

Tripwire debuts pentesting and industrial cybersecurity assessment services

Tripwire debuted its penetration testing and industrial cybersecurity assessment services at RSA Conference.

The Penetration Testing Assessment leverages highly skilled cybersecurity experts who discover and then exploit vulnerabilities to assess the security of an organization's IT environment.

It covers critical assets such as network services and configuration, web application, wireless infrastructure, client-side and internal infrastructure, and social engineering and physical security. It examines how authentication and data traffic flows throughout the network in order to establish the roles of various systems within the network, how different systems support the business functions of the organization, and how communication moves between a system and its users, providing information needed to design protective control mechanisms.

The Industrial Cybersecurity Assessment provides specialized evaluation of vulnerabilities in industrial control system (ICS) environments, taking into account the operational technology (OT) requirements of utility, manufacturing, oil and gas, and critical infrastructure operators.

To identify exposures in industrial environments, Tripwire's team of security professionals review data from automated vulnerability scanners, proprietary tools and manual assessments.

Tripwire can assess the following for vulnerabilities without disrupting operations: energy management systems (EMS), Supervisory Control and Data Acquisition (SCADA) systems, Real-time Control System (RCS) architecture, distributed control systems (DCS), programmable logic controllers (PLCs), and network devices.

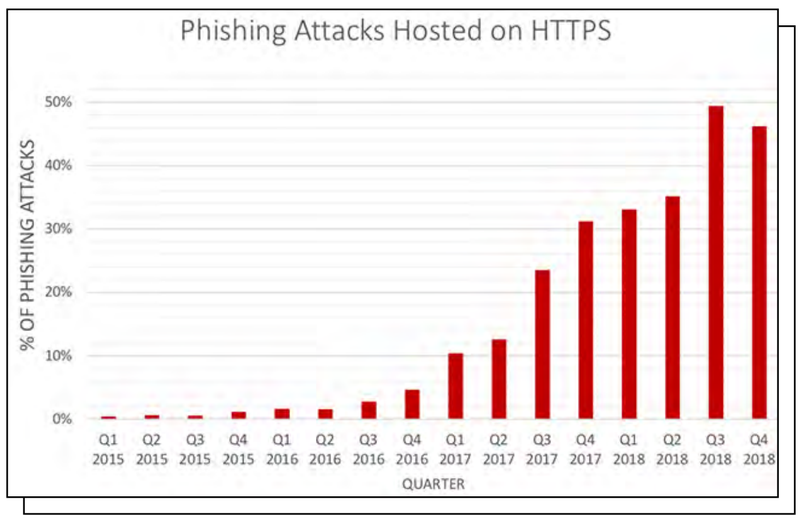
Phishers shift efforts to attack SaaS and webmail services

According to the APWG's Q4 2018 Phishing Activity Trends Report, the number of confirmed phishing sites declined as 2018 proceeded. The total number of phishing sites detected by APWG in 4Q was 138,328 – down from 151,014 in Q3, 233,040 in Q2, and 263,538 in Q1.

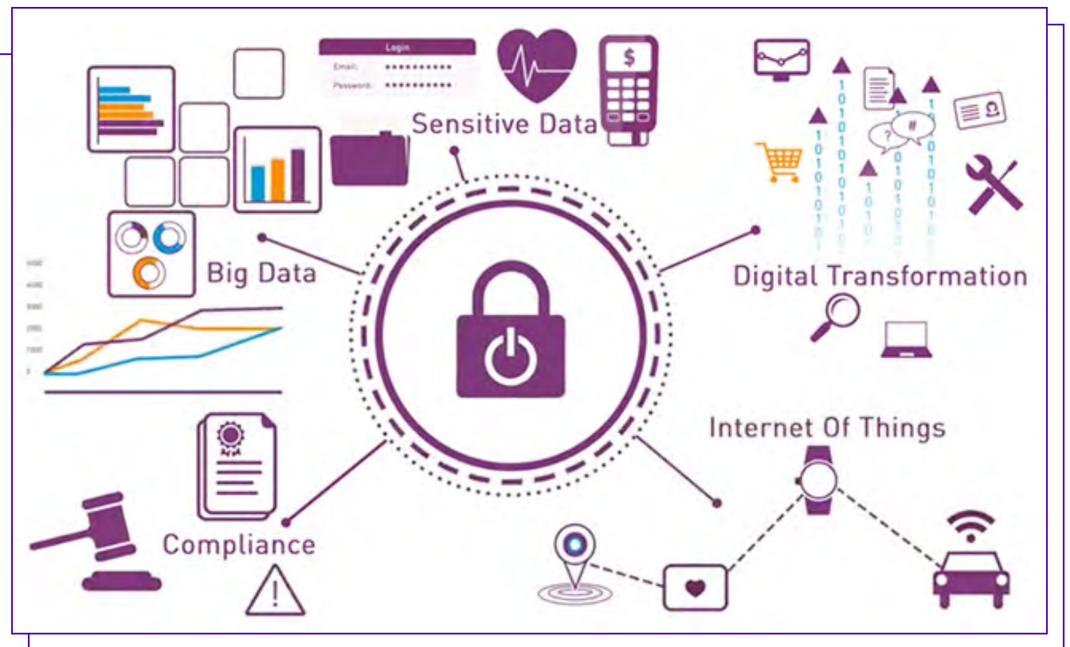
This general decline in the number of phishing campaigns as the year went on may have been a consequence of anti-phishing efforts – and/or the result of criminals shifting to more specialized and lucrative forms of e-crime than mass-market phishing.

Phishing that targeted SaaS and Webmail services jumped from 20.1 percent of all attacks in Q3 to almost 30 percent in Q4. Attacks against cloud storage and file hosting sites continued to drop, decreasing from 11.3 percent of all attacks in Q1 2018 to 4 percent in Q4 2018.

Researchers at APWG member PhishLabs observed that in the final quarter of 2018, the number of phishing attacks hosted on Web sites that have HTTPS and SSL certificates declined for the first time in history.



Gemalto expands cloud-based Hardware Security Module solutions



Gemalto, the world leader in digital security, announced the availability of three new cloud-based Hardware Security Module (HSM) services.

HSM On Demand for CyberArk works seamlessly with CyberArk's Privileged Access Security Solution, providing private key protection and strong entropy for key generation for system keys. By securing the master key and ensuring that it is hosted in a secure vault, HSM On Demand for CyberArk mitigates the risk of the master key being exposed or compromised.

HSM On Demand for Hyperledger provides trust for blockchain transactions by securing the cryptographic keys that sign them. It protects digital wallets, while ensuring keys are readily available in the cloud once access is granted. The service provides high assurance security in data centers and the cloud, enabling multi-tenancy of blockchain identities per partition as proof of transaction and for auditing requirements. It also delivers performance improvements resulting from off-loading cryptographic operations from application servers to the HSM on Demand service.

HSM for Oracle TDE (Transparent Data Encryption) solves the challenge presented by locally stored encryption keys by protecting them with a master key, stored in a separate service key vault. This ensures that only authorized services are allowed to request the local key to be decrypted. If an attacker steals the database, it is encrypted and inaccessible, since the attacker does not have access to the keys that are securely stored on the HSM.

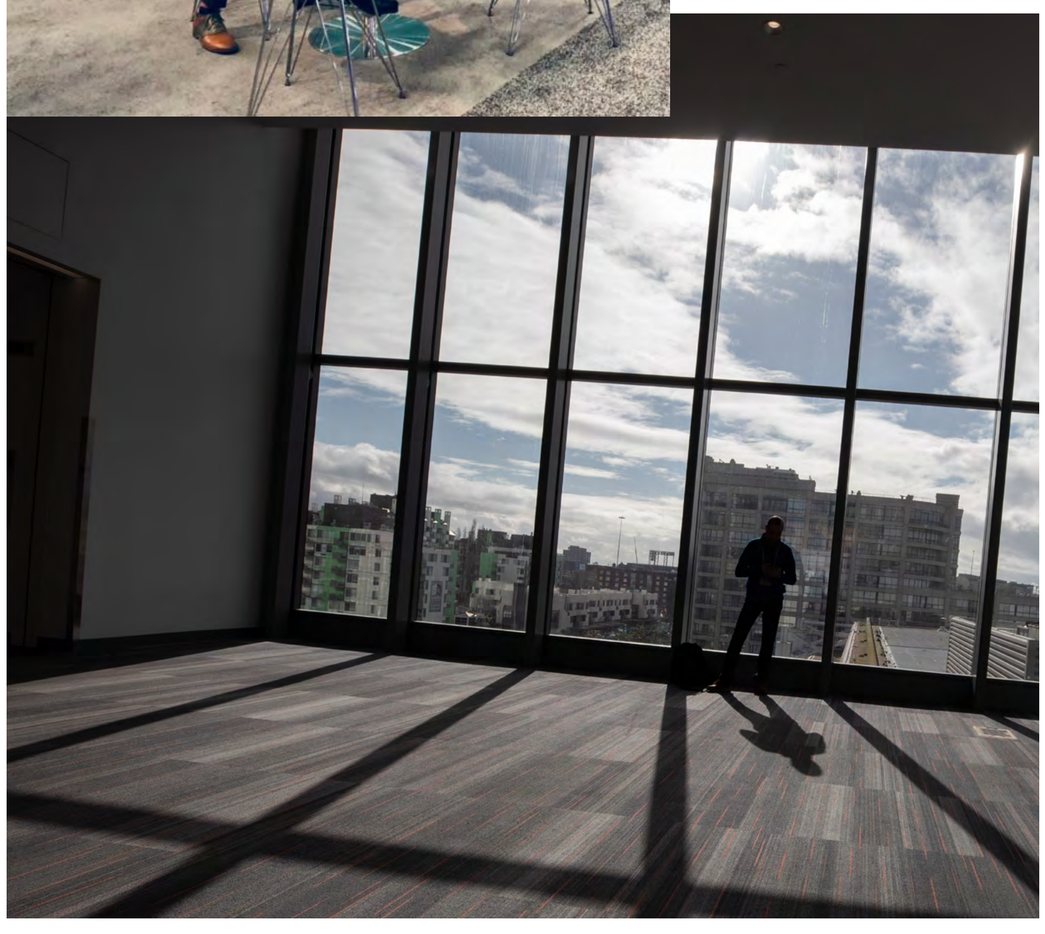
Each service is available through the SafeNet Data Protection on Demand platform.

SecBI launches new solution to help MSSPs maximize their productivity and scalability

SecBI announced an automated threat detection and response solution designed to help managed security service providers (MSSPs) maximize their productivity and scalability.

The SecBI MSSP offering automates both threat hunting, based on comprehensive network traffic analysis, and breach response. SecBI provides full scope detection, creating a comprehensive view of each cyber incident by combining disparate alerts, events, and logs into a single narrative that shows all the affected entities and kill chain. Finally, the solution delivers gap analysis that identifies network security blind spots and implements fixes.

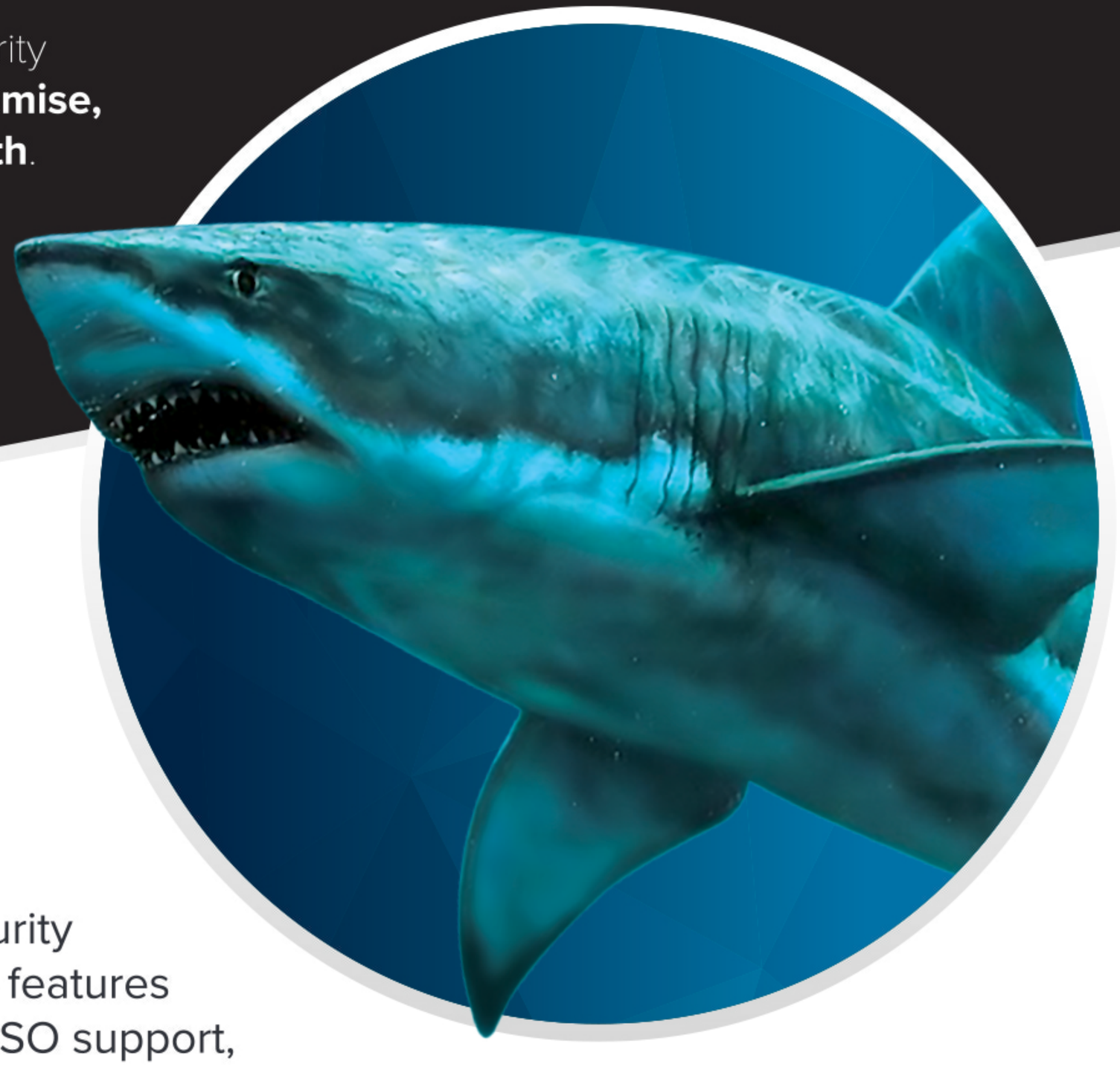
#RSAC 2019 gallery



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.

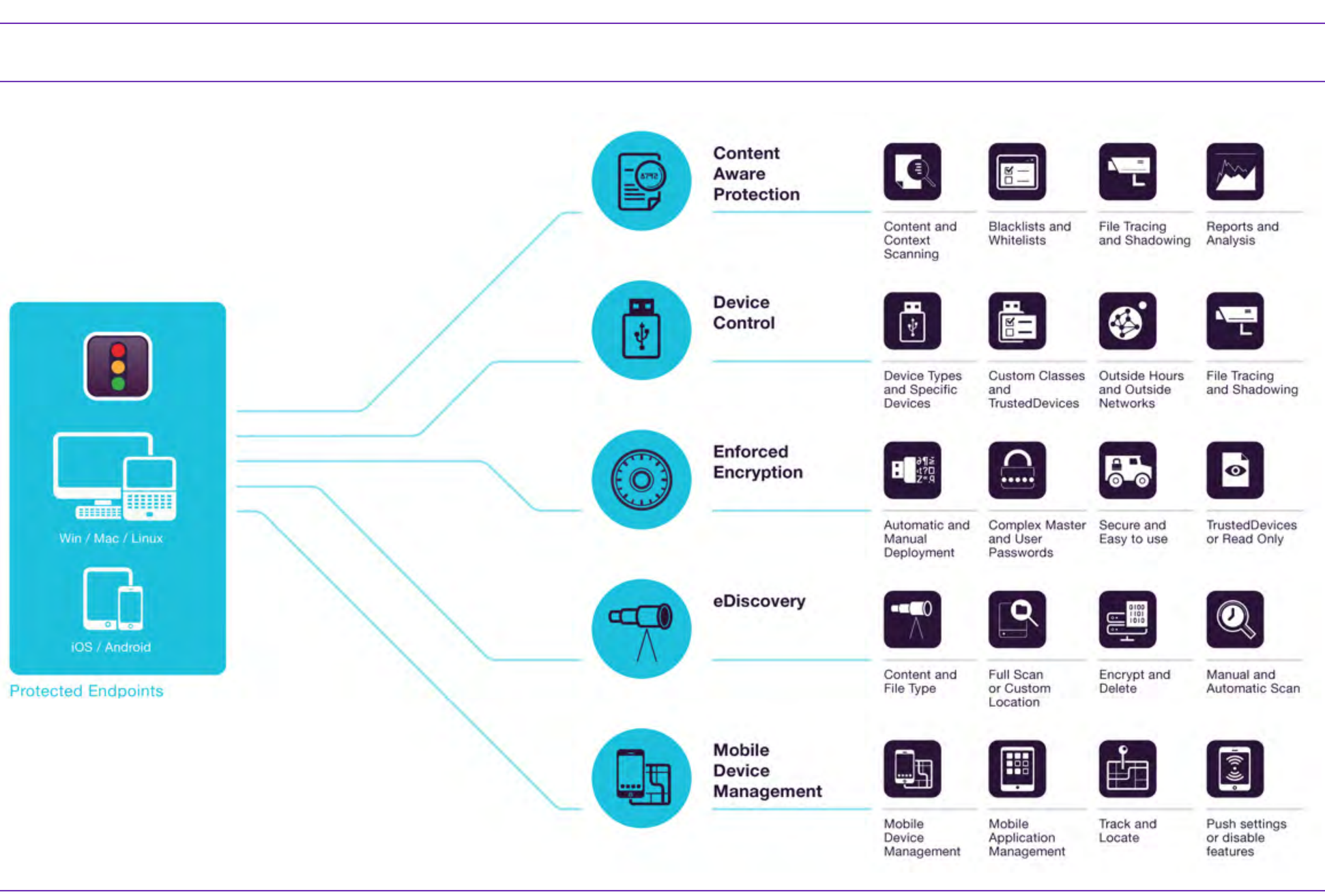


Proof-Based Scanning™

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



CoSoSys launches Endpoint Protector 5.2.0.5

CoSoSys announced Endpoint Protector 5.2.0.5, a new release of its award-winning Data Loss Prevention solution.

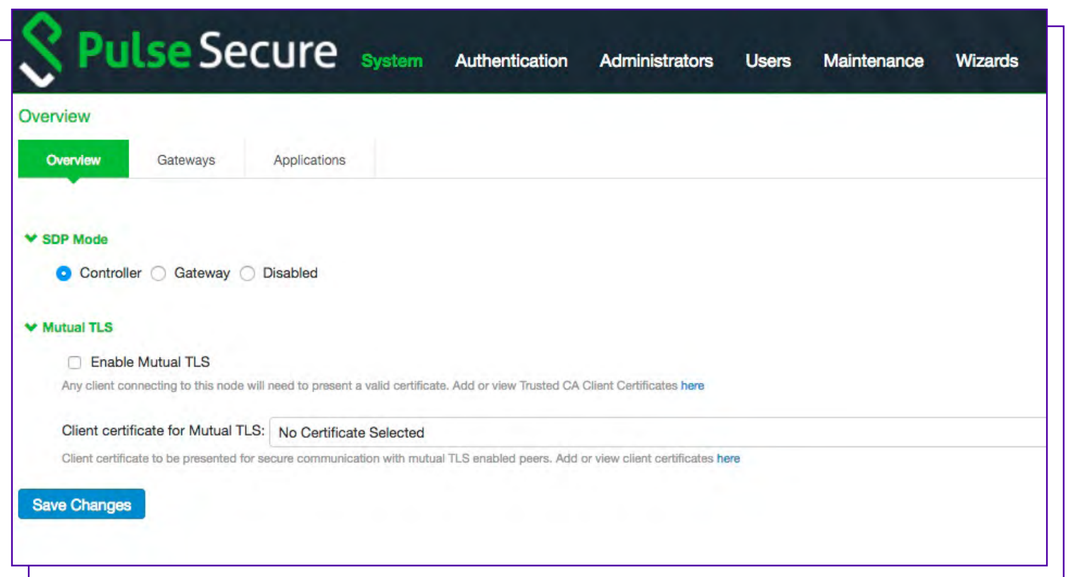
The latest update introduces a brand-new feature – the Deep Packet Inspection technology available for macOS and embedded into the Endpoint Protector client intercepts all file transfers through web browsers. With this feature now it is possible to monitor the destination of a file, as well as to whitelist and blacklist specific URLs. Whitelisting allows file transfers only to specific domains and URLs, while with the blacklisting option access to specific websites can be blocked.

In the latest update, the redesigned Directory Services section provides a greater flexibility, and it is easier to work with and pull information from the desired entities.

The Contextual Detection feature has been extended in Endpoint Protector 5.2.0.5 and now it is possible to include file types and file sizes in contextual rules.

Organizations subject to various rules and regulations (e.g.: cross-border regulations) now have Samba support for the File Shadow Repository feature. Besides, this functionality is also useful when the aim is to externalize File Shadows to a different network share in order to keep Endpoint Protector functioning at optimal parameters, without the load of unnecessary files.

Pulse Secure delivers secure access for hybrid IT with SDP solutions



Pulse Secure announced the integration of SDP (Software Defined Perimeter) architecture within its Secure Access platform and the inclusion of Pulse SDP as an add-on within its award-winning Access Suite.

Pulse Secure Access Suite provides remote, mobile, cloud, network and application security with comprehensive VPN, Mobile Device Management (MDM), Single Sign-on (SS0), endpoint and IOT device visibility, Network Access Control (NAC) and virtual Application Delivery Controller (ADC) capabilities.

Pulse SDP complements this integrated solution set by offering direct device to application/ resource secure connectivity only after successful user, device and security state verification including geo location and behavior-based anomaly detection. As a result, organizations gain seamless accessibility while streamlining access provisioning, improving performance and reducing the visible attack surface. More so, organizations gain greater economies and a non-disruptive way to readily implement SDP functionality when, where and how they require.

By offering a flexible path to SDP, the company extends its foundation of Zero Trust access for hybrid IT and provides enterprises and service providers unrivaled provisioning simplicity, security posture fortification and lower total cost of ownership.

Eclypsium and Intel offer new silicon-enabled security solutions

Eclypsium announced a collaboration with Intel to help organizations manage the entire firmware attack surface. Together with Intel, Eclypsium helps enterprise IT and cloud service providers construct a more secure foundation for computing by pairing security capabilities built-in to Intel silicon with advanced defenses against firmware threats.

Intel Security Essentials provide a built-in foundation for improved security features and are available across Intel processor lines. They enable security professionals to help protect the platform and the data and to build applications with security features in a consistent way.

The Eclypsium Platform, now generally available, builds upon Intel's foundation by analyzing the system configuration and ensuring the latest firmware is deployed. With Eclypsium, the end user can see the status of their firmware patch levels, gain visibility into firmware misconfigurations, and validate the integrity of Intel systems as part of the supply chain.

IBM X-Force Red will use Onapsis ERP technology to help organizations uncover critical vulnerabilities

Onapsis, the global leaders in ERP cybersecurity and compliance, announced IBM Security's team of veteran hackers, X-Force Red, will use its ERP technology to help organizations identify exploitable vulnerabilities in their business-critical (SAP and Oracle) applications.

Customers can access X-Force Red's services through the X-Force Red Portal, the team's cloud-based communications and collaboration platform. Using the X-Force Red Portal, customers can sign up for tests and assessments, check their status, view findings as they are uncovered, view remediation recommendations, and communicate directly with X-Force Red testers, eliminating time-consuming back and forth and the manual sharing of spreadsheets.

X-Force Red delivers vulnerability assessment and security testing programs that focus on uncovering vulnerabilities across applications, hardware, personnel, internet-connected devices, networks, cars, ATMs, blockchain and just about everything else.

The team is comprised of veteran hackers who apply the same tools, techniques, practices and mindset as attackers, uncovering exploitable vulnerabilities that may lead criminals to the crowned jewels.

This collaboration further highlights Onapsis' increased effort on growing the global ERP security partner ecosystem. Onapsis also works closely with the IBM Security Services group for protecting, continuous monitoring, addressing compliance and enabling cloud migrations of some of the world's largest organizations.

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

Anomali, Flashpoint, and Intel 471 join Verodin to launch Threat Actor Assurance Program

Verodin announced its new Threat Actor Assurance Program (TAAP), which will combine industry-leading threat intelligence from Anomali, Flashpoint, and Intel 471 with Verodin's proven capability to validate cybersecurity effectiveness.

This powerful program will deliver actionable intelligence on how an organization's defenses will perform against the threat actors specifically targeting them.

As part of the program, Verodin is introducing its Threat Actor Assurance Module (TAAM). With the release of TAAM, the company is providing customers with the ability to determine if threat actors could get through their defenses before the actual attack by making threat intelligence actionable. TAAM validates a customer's defensive stack's capabilities to prevent, detect, and alert on both indicators of compromise and tactics, techniques, and procedures (TTPs) – including the MITRE ATT&CK framework.

Organizations using Verodin TAAM will also be able to determine if they have gaps in control visibility or misconfigurations that could aid in a threat actor compromise. Once an organization has a baseline understanding of their coverage, they can tune and optimize their security stack to reach a higher level of assurance.

NSA released Ghidra, its internal reverse engineering tool

The National Security Agency (NSA) has released Ghidra, a free and cross-platform software reverse engineering tool suite used internally by the intelligence agency. They are also planning on releasing the tool's source code on GitHub soon.

"In support of NSA's Cybersecurity mission, Ghidra was built to solve scaling and teaming problems on complex SRE [software reverse engineering] efforts, and to provide a customizable and extensible SRE research platform. NSA has applied Ghidra SRE capabilities to a variety of problems that involve analyzing malicious code and generating deep insights for SRE analysts who seek a better understanding of potential vulnerabilities in networks and systems," the agency explained.

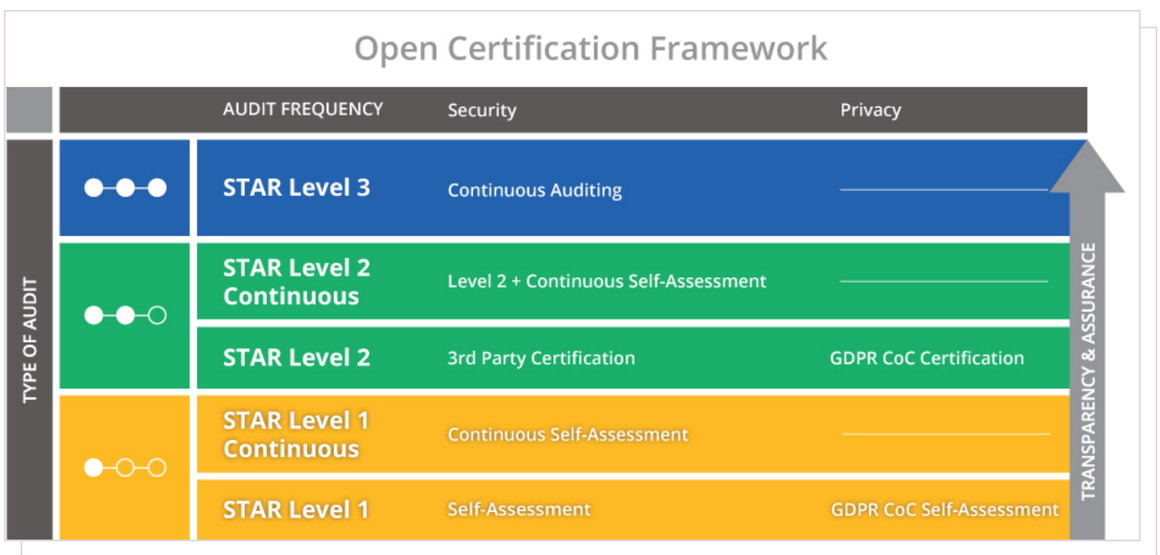
"[Ghidra] includes a suite of full-featured, high-end software analysis tools that enable users to analyze compiled code on a variety of platforms including Windows, Mac OS, and Linux. Capabilities include disassembly, assembly, decompilation, graphing, and scripting, along with hundreds of other features. Ghidra supports a wide variety of process instruction sets and executable formats and can be run in both user-interactive and automated modes."

Users can develop their own plugins, scripts and analyzers and the NSA hopes that, once its source code is released, the wider community of software engineers and malware analysts will contribute to its development by reporting bugs, submitting patches, reviewing the code and proposing new features.

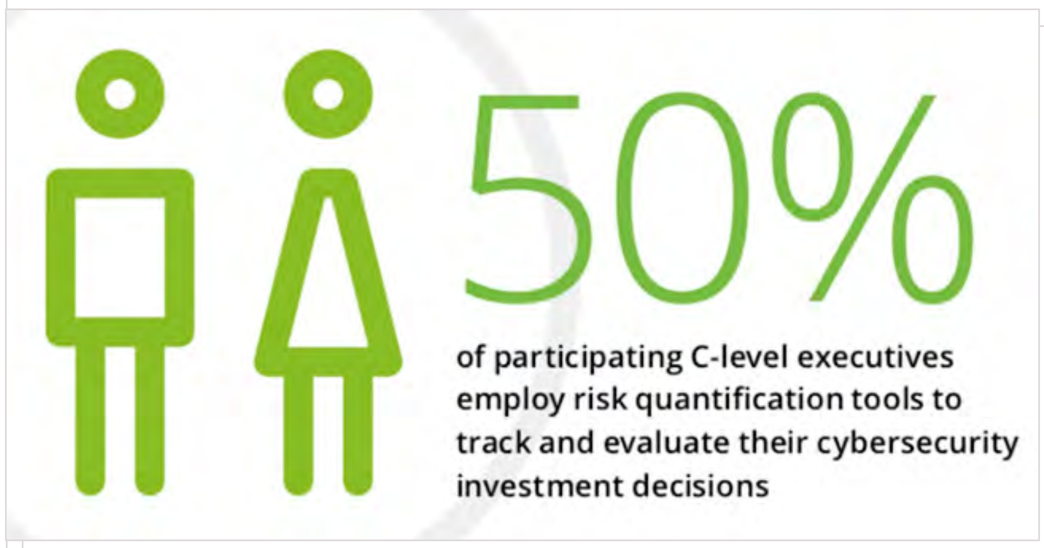
CSA launches compliance assessment program for cloud service providers

The Cloud Security Alliance (CSA) announced STAR Continuous Self Assessment, the first release of an evolving continuous-compliance assessment program for cloud services that gives cloud service providers (CSPs) the opportunity to align their security validation capabilities with cloud security compliance and certification on an ongoing basis.

STAR consists of three levels of assurance (Self-Assessment, Third-Party Certification and Continuous Auditing), based upon the CSA Cloud Controls Matrix (CCM), the Consensus Assessments Initiative Questionnaire (CAIQ), and the CSA Code of Conduct for GDPR Compliance. Future releases will be Level 2 Extended Certification with Continuous Self-Assessment and Level 3 Continuous Certification.

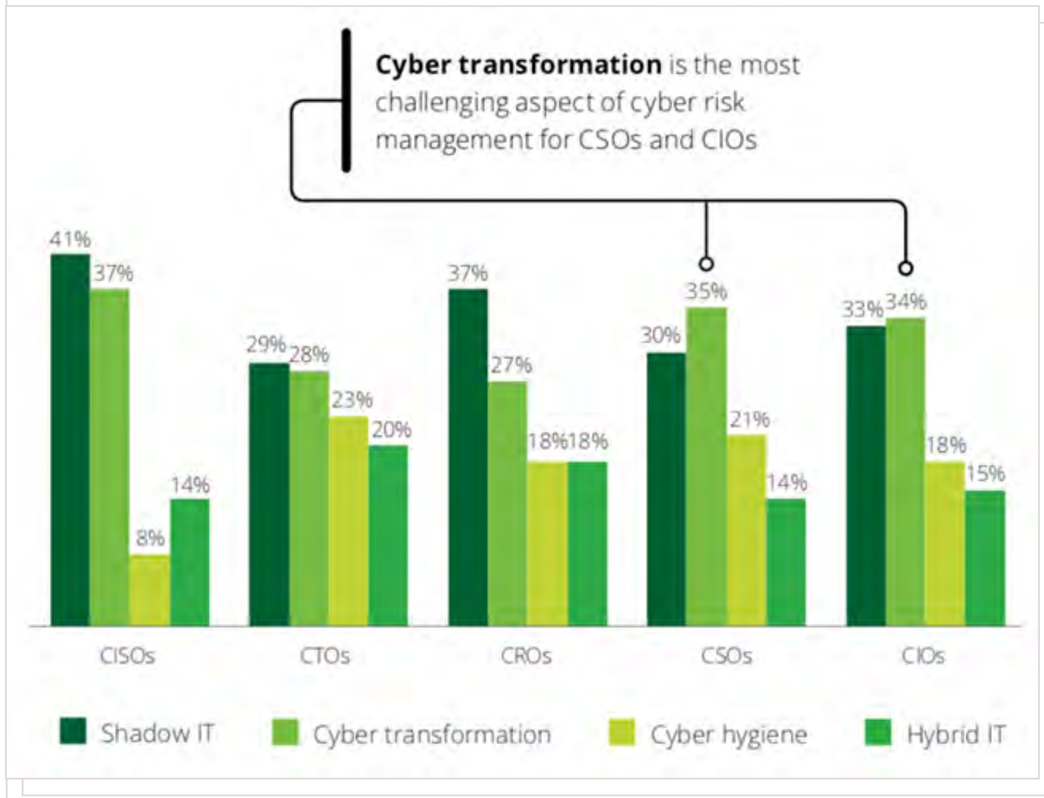


How are execs tackling cyber risk that comes with digital transformation?



Deloitte Cyber surveyed 500 C-suite executives who have responsibility for cyber security to explore their challenges in leading the transformation from legacy environments, disconnected data sources, identity systems, and governance issues, to name a few.

Results from the survey indicate that many cyber organizations are challenged by their ability to help better prioritize cyber risk across the enterprise (16 percent), followed closely behind by lack of management alignment on priorities and adequate funding, each at 15 percent.



Survey findings:

- While organizations are prioritizing digital transformation, only 14 percent of cyber budgets are allocated to securing transformation efforts
- Less than 20 percent of organizations have security liaisons embedded within business units to foster greater collaboration, innovation and security
- Organizations are turning to third parties to manage certain facets of their cyber operations.
- There's a disconnect between the majority (85 percent) of the survey respondents who indicate that they are using Agile/DevOps in application development and then ranking DevSecOps lowest (11 percent) on the cyber defense priorities and investments areas, which may explain why 90 percent of organizations surveyed experienced disclosures of sensitive production data within the past year.
- Data integrity (35 percent) was the top ranked cybersecurity threat survey respondents were most concerned about, followed by unintended actions of well- meaning employees (32 percent) resulting in a negative event and technical vulnerabilities (31 percent).

If an organization has been breached, it's more likely to be targeted again

FireEye released the Mandiant M-Trends 2019 report, which shares statistics and insights gleaned from Mandiant investigations around the globe in 2018.

Key findings:

Dwell time decreasing as organizations improve detection capabilities – In 2017, the median duration between the start of an intrusion and the identification by an internal team was 57.5 days. In 2018 this duration decreased to 50.5 days. While organizations are getting better and faster at discovering breaches internally, rather than being notified by an outside source such as law enforcement, there is also a rise in disruptive, ransom, or otherwise immediately visible attacks.

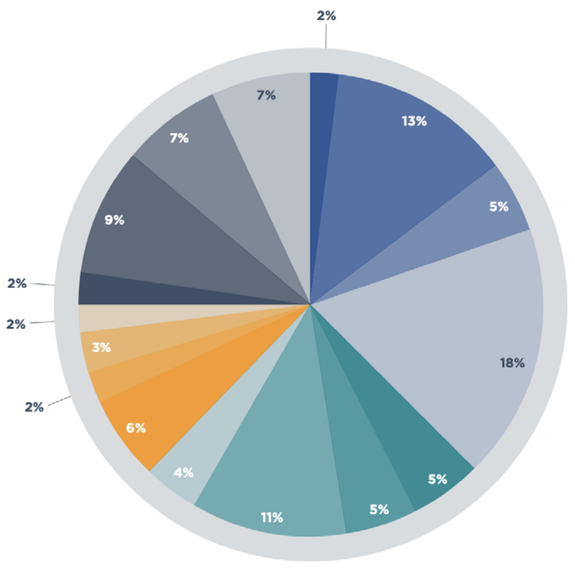
Nation-state threat actors are continuing to evolve and change – Through ongoing tracking of threat actors from North Korea, Russia, China, Iran, and other countries, FireEye has observed these actors continually enhancing their capabilities and changing their targets in alignment with their political and economic agendas.

Attackers are becoming increasingly persistent – FireEye data provides evidence that organizations which have been victims of a targeted compromise are likely to be targeted again. Global data from 2018 found that 64 percent of all FireEye managed detection and response customers who were previously Mandiant incident response clients were targeted again in the past 19 months by the same or similarly motivated attack group, up from 56 percent in 2017.

Many attack vectors used to get to targets, including M&A activity – Attacker activity touches countries across the globe. Among them, FireEye observed an increase in compromises through phishing attacks during mergers & acquisitions (M&A) activity. Attackers are also targeting data in the cloud, including cloud providers, telecoms, and other service providers, in addition to re-targeting past victim organizations.

MANAGED DETECTION AND RESPONSE CUSTOMERS RETARGETED IN 2018 (BY INDUSTRY)

Industries Targeted			
Defense Industrial Base	2%	IT	6%
Education	13%	Legal	2%
Energy	5%	Manufacturing	3%
Finance	18%	Media	2%
Food and Beverage	5%	Mining	2%
Government	5%	Pharmaceutical	9%
Health	11%	Retail and Hospitality	7%
Industrial	4%	Telecommunications	7%



Ongoing global cyber espionage campaign broader than previously known

A detailed analysis of code and data from a command-and-control server responsible for the management of the operations, tools and tradecraft behind the Operation Sharpshooter campaign has revealed evidence that this global cyber espionage campaign is more extensive in complexity, scope and duration of operations.

The analysis led to identification of multiple previously unknown command-and-control centers, and suggest that Sharpshooter began as early as September 2017, targeted a broader set of organizations, in more industries and countries and is currently ongoing.

Analysis of the new evidence has exposed striking similarities between the technical indicators, techniques and procedures exhibited in these 2018 Sharpshooter attacks, and aspects of multiple other groups of attacks attributed by the industry to the Lazarus Group. This includes, for example, the Lazarus group's use of similar versions of the Rising Sun implant dating back to 2017, and source code from the Lazarus Group's infamous 2016 backdoor Trojan Duuzer.

#RSAC 2019 gallery