[+] (IN)SECUREMagazine

05 | 2018

ISSUE 57.5

#RSAC 2018

Introducing

Two new free services!

CertView

qualys.com/certview-free

Full inventory of your Internet-facing certificates

See your SSL/TLS configuration grades with recommended fixes

Identify the certificate issuer

Track certificate expiration

Instantly upgrade to include internal certs

CloudView

qualys.com/cloudview-free

Total visibility into your public cloud workloads & infrastructure

See all of your cloud assets from a single-pane interface

Monitor your clouds' users, instances, networks, storage, databases and their relationships

Instantly upgrade to run security assessments on your cloud assets

Qualys®

© 2018 Qualys, Inc. All rights reserved.

RSA Conference, the world's leading information security conferences and expositions, concluded its 27th annual event in San Francisco on April 20th. More than 42,000 attendees experienced keynote presentations, peer-to-peer sessions, track sessions, tutorials, expo floors and seminars during the course of the week focused on topics such as artificial intelligence, data privacy, gamification, the history of technology and innovation, among others.

"We succeeded, in a week filled with knowledge sharing, collaboration and the exchange of innovative ideas among the industry's elite," said Linda Gray Martin, Director & General Manager of RSA Conference.

Sponsors of our coverage from RSA Conference 2018

DIAMOND SPONSOR

Qualys.

GOLD SPONSOR

ANOMALI

SILVER SPONSORS

ABSOLUTE
CAPSULE8
COSOSYS
Fortanix
MICRO FOCUS
NEHEMIAH SECURITY
onapsis
silent circle
THREATQUOTIENT
VERA

BRONZE SPONSORS

ACALVIO
Cryptshare
Making e-mail better

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

Qualys brings web application security to DevOps

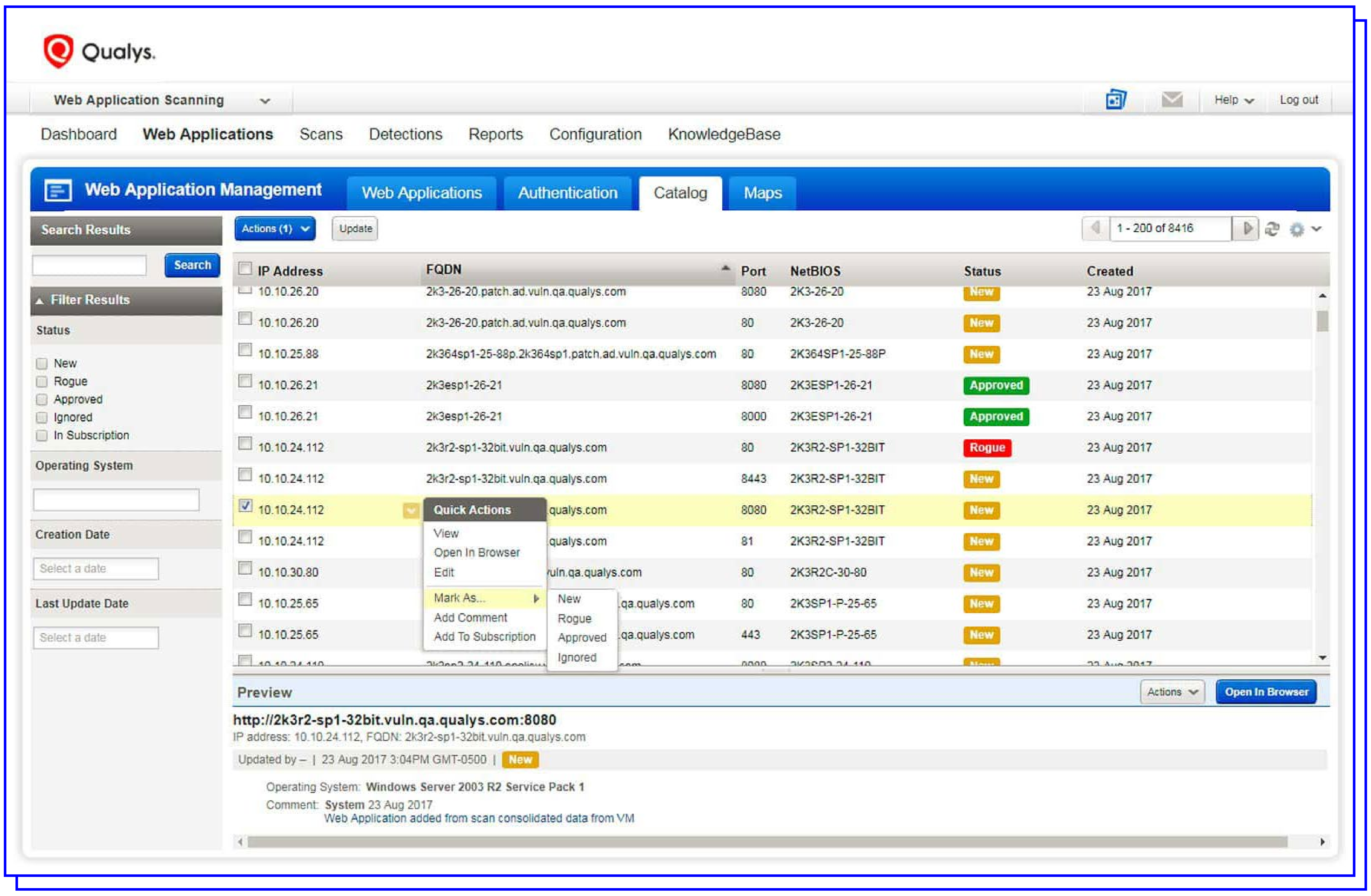
Qualys announced new functionality in its web application security offerings that helps teams automate and operationalize global DevSecOps throughout the Software Development Lifecycle (SDLC), drastically reducing the cost of remediating application security flaws prior to production.

Qualys Web Application Scanning (WAS) 6.0 now supports Swagger version 2.0, a new native plugin for Jenkins for automated vulnerability scanning of web applications, and the new Qualys Browser Recorder.

Qualys WAS 6.0 and new capabilities include:

Scanning of Swagger-based REpresentational State Transfer (REST) APIs

In addition to scanning Simple Object Access Protocol (SOAP) web services, Qualys WAS now leverages the Swagger specification for testing REST APIs. Users need only ensure the Swagger version 2.0 file (JSON format) is visible to the scanning service, and the APIs will automatically be tested for common application security flaws.



	IP Address	FQDN	Port	NetBIOS	Status	Created
□	10.10.26.20	2k3-26-20.patch.ad.vuln.qa.qualys.com	8080	2K3-26-20	New	23 Aug 2017
□	10.10.26.20	2k3-26-20.patch.ad.vuln.qa.qualys.com	80	2K3-26-20	New	23 Aug 2017
□	10.10.25.88	2k364sp1-25-88p.2k364sp1.patch.ad.vuln.qa.qualys.com	80	2K364SP1-25-88P	New	23 Aug 2017
□	10.10.26.21	2k3esp1-26-21	8080	2K3ESP1-26-21	Approved	23 Aug 2017
□	10.10.26.21	2k3esp1-26-21	8000	2K3ESP1-26-21	Approved	23 Aug 2017
□	10.10.24.112	2k3r2-sp1-32bit.vuln.qa.qualys.com	80	2K3R2-SP1-32BIT	Rogue	23 Aug 2017
□	10.10.24.112	2k3r2-sp1-32bit.vuln.qa.qualys.com	8443	2K3R2-SP1-32BIT	New	23 Aug 2017
☑	10.10.24.112	qualys.com	8080	2K3R2-SP1-32BIT	New	23 Aug 2017
□	10.10.24.112	qualys.com	81	2K3R2-SP1-32BIT	New	23 Aug 2017
□	10.10.30.80	uln.qa.qualys.com	80	2K3R2C-30-80	New	23 Aug 2017
□	10.10.25.65	qa.qualys.com	80	2K3SP1-P-25-65	New	23 Aug 2017
□	10.10.25.65	qa.qualys.com	443	2K3SP1-P-25-65	New	23 Aug 2017

http://2k3r2-sp1-32bit.vuln.qa.qualys.com:8080
IP address: 10.10.24.112, FQDN: 2k3r2-sp1-32bit.vuln.qa.qualys.com
Updated by – | 23 Aug 2017 3:04PM GMT-0500 | New

Operating System: **Windows Server 2003 R2 Service Pack 1**
Comment: **System** 23 Aug 2017
Web Application added from scan consolidated data from VM

Jenkins plugin

The Qualys WAS Jenkins plugin empowers DevOps teams to build application vulnerability scans into their existing Continuous Integration/ Continuous Delivery (CI/CD) processes. By integrating scans in this manner, application security testing is accomplished earlier in the SDLC to catch and eliminate security flaws thereby significantly reducing the cost of remediation compared to doing so later in the SDLC.

Qualys Browser Recorder

This new Chrome extension allows users to record web browser activity and save the scripts for repeatable, automated testing. Scripts are played back in Qualys WAS, allowing the scanning engine to successfully navigate through complex authentication and business workflows. The Qualys Browser Recorder extension is free and available to anyone (not just Qualys customers) via the Chrome Web Store.

"As companies move their internal apps to the cloud and embrace new technologies, web app security must be integrated into the DevOps process to safeguard data and prevent breaches," said Philippe Courtot, chairman and CEO, Qualys.

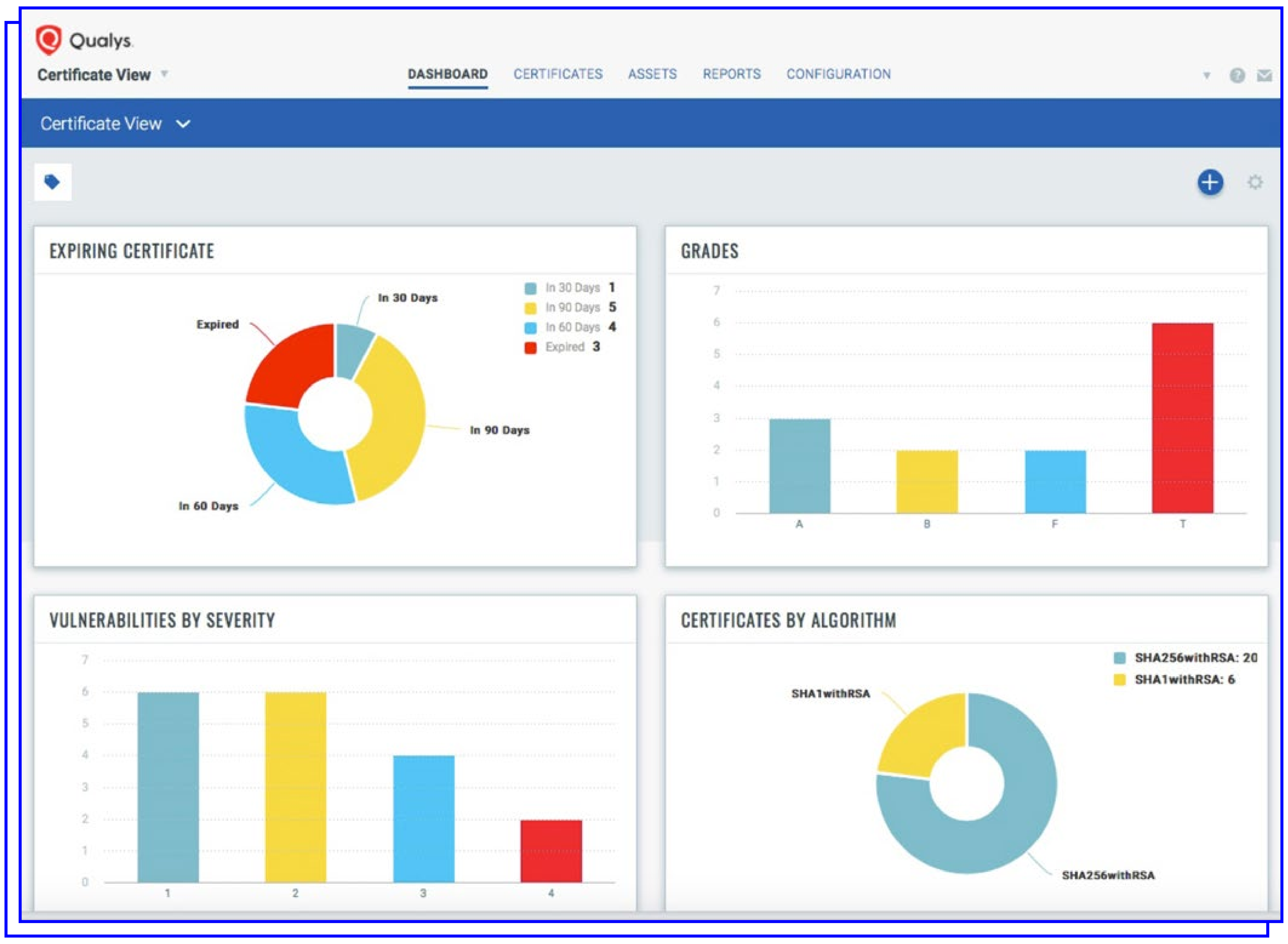
Qualys is helping customers streamline and automate their DevSecOps through continuous visibility of security and compliance across their applications and REST APIs. With the latest WAS features, customers now can make web application security an integral part of their DevOps processes, avoiding costly security issues in production.

Free Qualys services give organizations visibility of their digital certs and cloud assets

Qualys announced two new free groundbreaking services: CertView and CloudView.

Harnessing the power and scalability of the Qualys Cloud Platform, Qualys CertView and CloudView enable organizations of all sizes to gain such visibility by helping them create a continuous inventory and assessment of their digital certificates, cloud workloads and infrastructure that is integrated into a single-pane view of security and compliance.

Qualys CertView



CertView helps customers inventory and assess certificates and underlying SSL/TLS configurations and vulnerabilities across external-facing assets to prevent downtime and outages, and to mitigate risks associated with expired or vulnerable SSL/TLS certificates and configurations.

It offers:

Certificate Discovery

Enabling Infosec and other teams to continuously scan global IT assets from the same console to discover every internet-facing certificate issued from any certificate authority.

Certificate Inventory

Enabling reduced administrative costs by bringing the entire certificate estate under central control with comprehensive visibility of all external certificates in use across DevSecOps, InfoSec and IT teams.

TLS Configuration Grades

CertView generates certificate instance grades (A, B, C, D, etc.) using SSL Labs' methodology that allows administrators to assess often-overlooked server SSL/TLS configurations without having to become SSL experts.

Continuous Monitoring

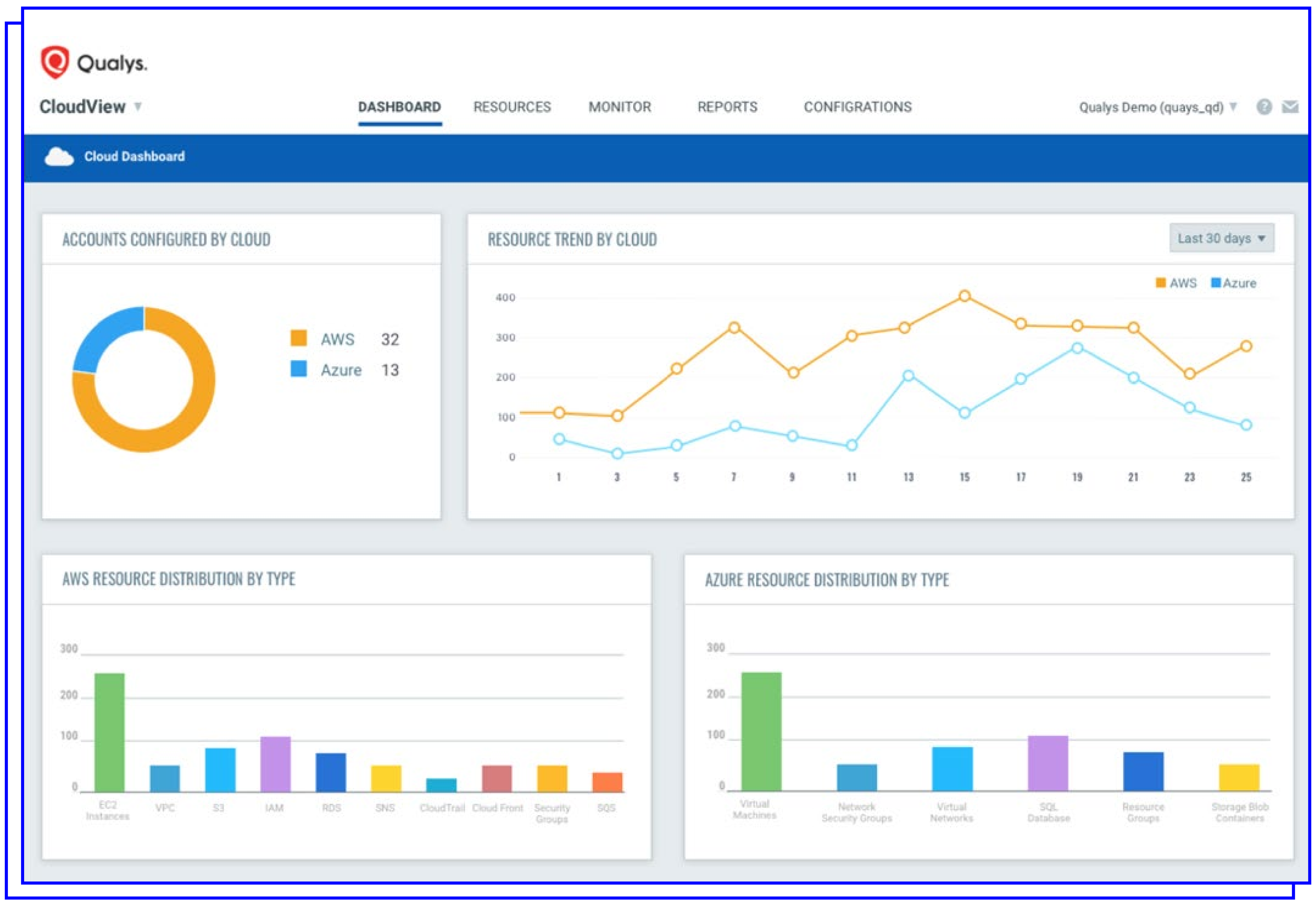
Automation built into the Qualys Cloud Platform identifies critical issues, weaknesses and vulnerabilities for DevSecOps, InfoSec and IT teams.

Reports and Dashboards

Dynamic dashboards provide teams with a holistic and contextual view of their external certificate estate, and power automatically created downloadable reports of certificate-related vulnerabilities, certificate expirations and non-compliant certificates across externally facing IT assets.

Customers can extend the power of these same features across their internal certificates by upgrading from Qualys CertView to Qualys Certificate Inventory (CRI) and Assessment (CRA) Apps.

Qualys CloudView



CloudView delivers customers topological visibility and insight about the security and compliance posture of their public cloud infrastructure for major providers including Amazon Web Services (AWS), Microsoft Azure and Google Cloud.

It offers:

Asset discovery and inventory

CloudView continuously discovers and tracks assets and resources — instances, virtual machines, storage buckets, databases, security groups, Access Control Lists, Elastic Load Balancers and users — across all regions, multiple accounts and multiple cloud platforms in one central place.

Complete comprehensive, multi-faceted searches

CloudView powers asset searches to help teams discover their threat posture based on attributes and relationships. It lets them find leaky storage buckets, ungoverned instances, and those scheduled for retirement. Complex lookups allow teams to identify assets that are at greater risk of attack, such as those that have high-severity vulnerabilities or that exist at the edge rather than inside the DMZ.

CloudView is free for up to three accounts per public cloud platform. Customers can instantly upgrade their subscription by adding Qualys Cloud Inventory (CI) and Cloud Security Assessment (CSA) Cloud Apps, which include:

Continuous security monitoring

Boosts the security of public clouds by identifying threats caused by misconfigurations, unwarranted access, and non-standard deployments. It automates security monitoring against industry standards, regulatory mandates and best practices to prevent issues like leaky storage buckets, unrestricted security groups, and crypto-mining attacks.

Insight and threat prioritization

Provides a 360-degree view of cloud assets' security posture, which includes cloud host vulnerabilities, compliance requirements and threat intelligence insights, so users can contextually prioritize remediation.

Quick identification of incident causes

Quickly uncovers the root cause of incidents. Simple yet powerful queries deliver search results across a complete cloud resource inventory that shows assets' configurations and complex associations, allowing teams to also identify similar assets and mitigate issues in a unified way.

Comprehensive DevOps protection

Powers automated security checks, identifies and eliminates issues, and standardizes deployment and formation templates to make production environments more secure. All features are supported via REST APIs for seamless integration with the CI/CD tool chain, providing DevSecOps teams with an up-to-date assessment of potential risks and exposure.

Illumio and Qualys integrate to deliver vulnerability-based micro-segmentation

Illumio announced new global vulnerability mapping capabilities on its Adaptive Security Platform. Vulnerability and threat data from the Qualys Cloud Platform is integrated with Illumio application dependency mapping to show potential attack paths in real time.

The integration between the Qualys Cloud Platform and Illumio delivers vulnerability maps, enabling organizations to see connections to vulnerabilities within and between applications. This new capability also includes an East-West exposure score that calculates how many workloads can potentially exploit vulnerabilities on applications.

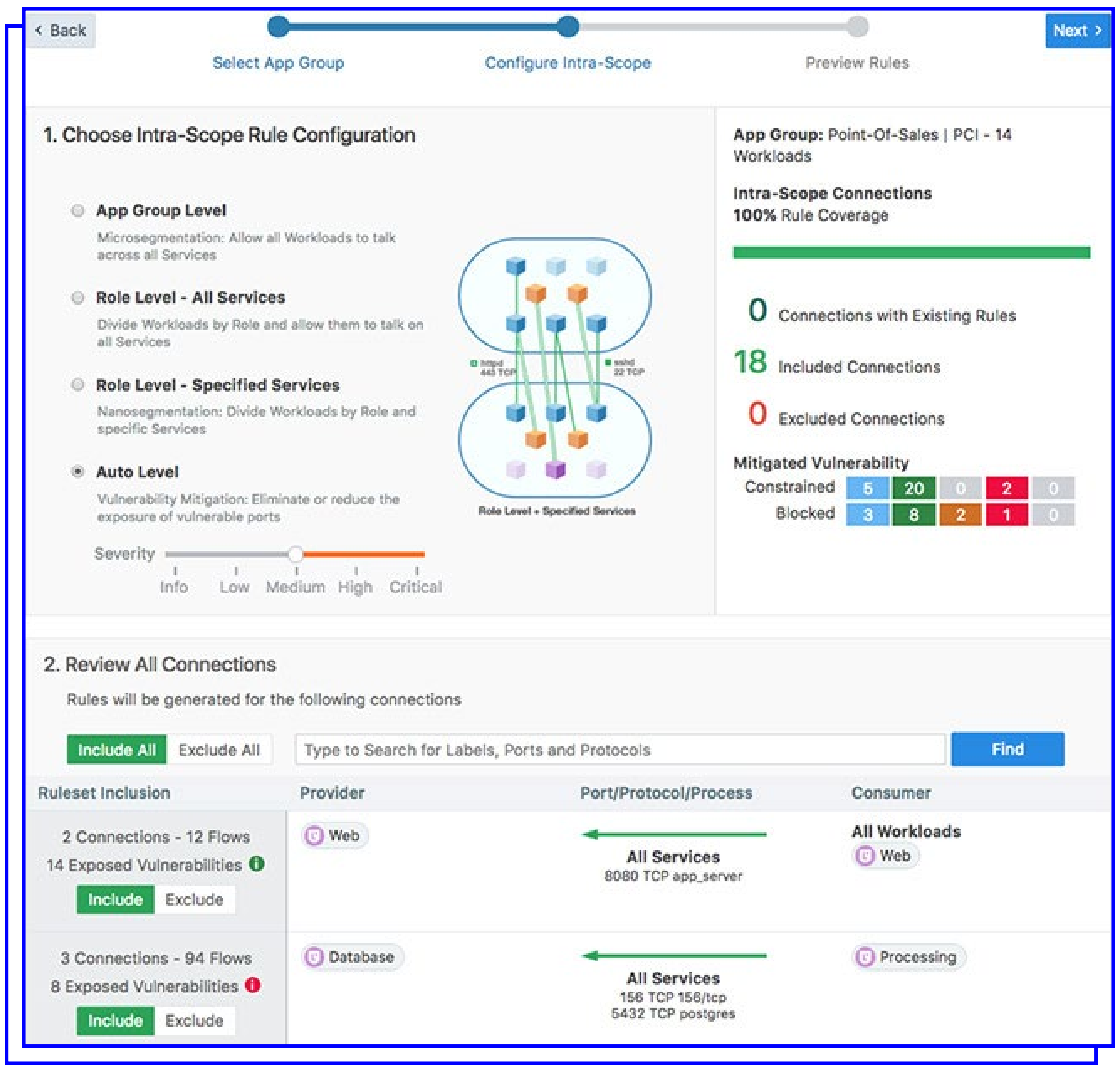
This integration can be used to generate micro-segmentation policies as compensating controls that reduce East-West exposure and to prioritize patching.

"Digital transformation leads to an explosion of connected environments where perimeter protection is no longer enough. The focus now needs to shift from securing network perimeters to safeguarding data spread across applications, systems, devices, and the cloud," said Philippe Courtot, CEO and Chairman of Qualys.

> The new Illumio integration with Qualys helps enterprises get visibility across hybrid environments and implement appropriate controls to protect assets from cyber threats, whether on premises or in the cloud.

Software vulnerabilities in applications have been the cause of recent headline-grabbing attacks and data breaches around the world, including WannaCry, NotPetya, and Apache Struts. Meltdown and Spectre are among other recent examples of vulnerabilities where potential exploitation could give attackers access to an environment – or to move laterally within data centers and clouds. Due to the growing scale of infrastructure and software vulnerabilities, organizations are unable to patch every vulnerability and may be unable to patch many critical vulnerabilities due to production freezes or for fear of breaking their applications.

> Vulnerability management is an invaluable tool in every security team's arsenal. With our Qualys Cloud Platform integration, organizations can see a map of how active, exposed vulnerabilities can potentially be exploited by a bad actor.
> _ Andrew Rubin, CEO of Illumio.



1. Choose Intra-Scope Rule Configuration

○ App Group Level
Microsegmentation: Allow all Workloads to talk across all Services

○ Role Level - All Services
Divide Workloads by Role and allow them to talk on all Services

○ Role Level - Specified Services
Nanosegmentation: Divide Workloads by Role and specific Services

● Auto Level
Vulnerability Mitigation: Eliminate or reduce the exposure of vulnerable ports

App Group: Point-Of-Sales | PCI - 14 Workloads

Intra-Scope Connections
100% Rule Coverage

0 Connections with Existing Rules
18 Included Connections
0 Excluded Connections

Mitigated Vulnerability

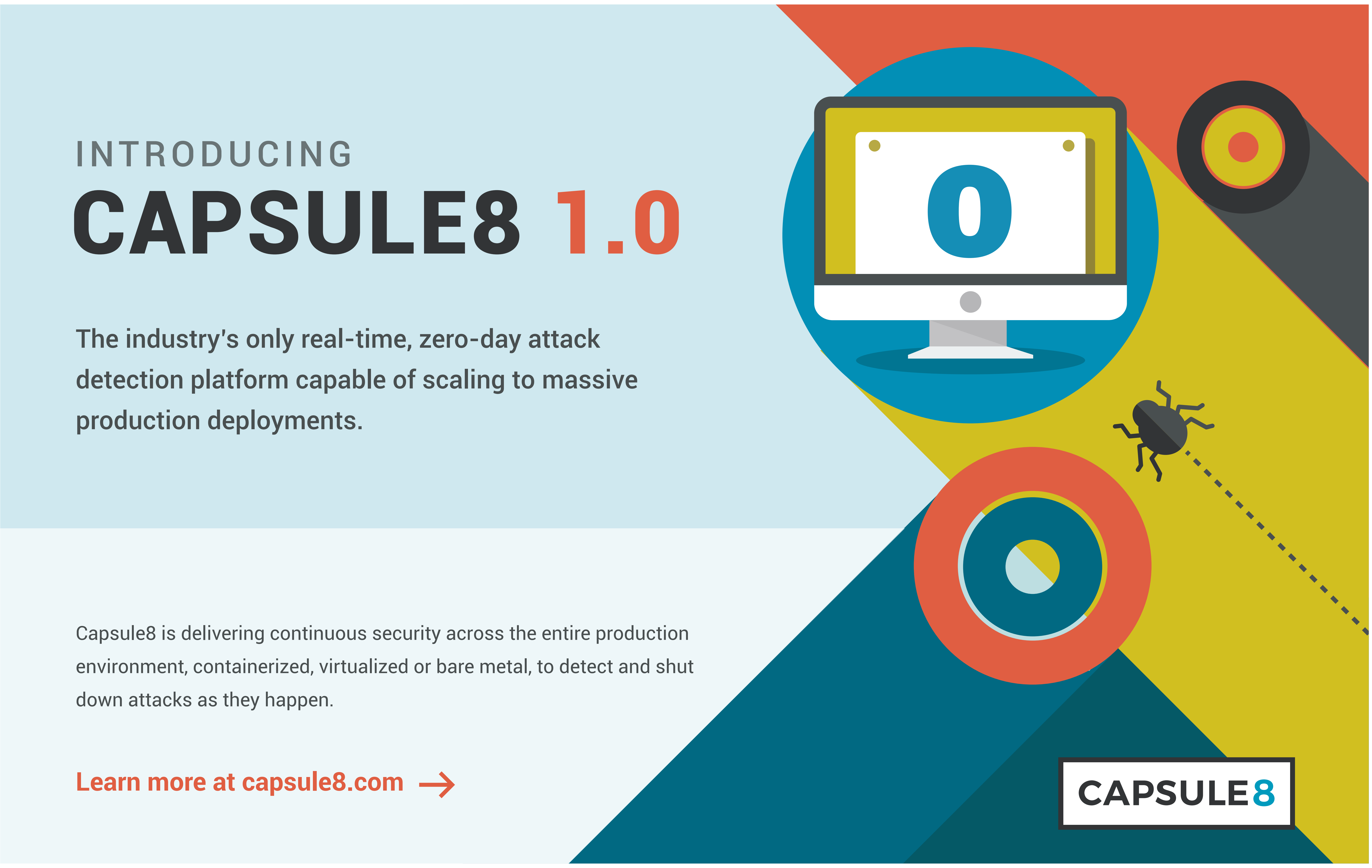
Constrained	5	20	0	2	0
Blocked	3	8	2	1	0

2. Review All Connections

Rules will be generated for the following connections

Ruleset Inclusion	Provider	Port/Protocol/Process	Consumer
2 Connections - 12 Flows 14 Exposed Vulnerabilities	Web	All Services 8080 TCP app_server	All Workloads Web
3 Connections - 94 Flows 8 Exposed Vulnerabilities	Database	All Services 156 TCP 156/tcp 5432 TCP postgres	Processing

#RSAC 2018 gallery



INTRODUCING
CAPSULE8 1.0

The industry's only real-time, zero-day attack detection platform capable of scaling to massive production deployments.

Capsule8 is delivering continuous security across the entire production environment, containerized, virtualized or bare metal, to detect and shut down attacks as they happen.

Learn more at capsule8.com →

CAPSULE8

Open-source library for improving security of AI systems

IBM researchers have created the Adversarial Robustness Toolbox, an open-source library to help researchers improve the defenses of real-world AI systems. It contains implementations of a number of attack and defense methods.

The library is written in Python, as it is the most commonly used programming language for developing, testing and deploying Deep Neural Networks.

“This first release of the Adversarial Robustness Toolbox supports DNNs implemented in the TensorFlow and Keras deep learning frameworks. Future releases will extend the support to other popular frameworks such as PyTorch or MXNet,” IBM pointed out and noted that, at the moment, the library is primarily intended to improve the adversarial robustness of visual recognition systems.

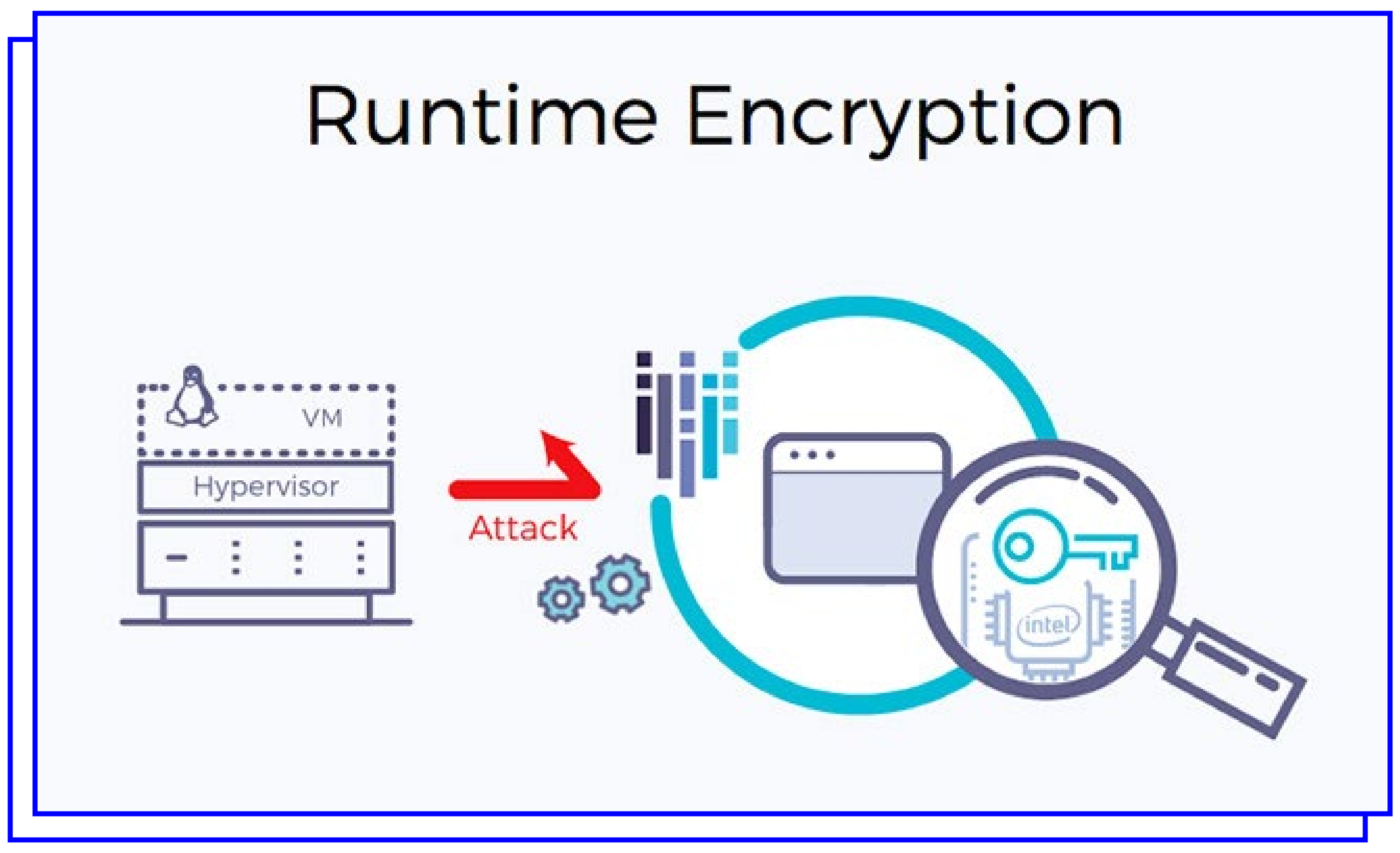
Future releases will include adaptations to other data modes (speech, text or time series).

Fortanix presented on protecting containerized apps with runtime encryption at RSAC 2018

Fortanix was selected to present in the session Protecting Containers from Host-Level Attacks at RSA Conference 2018 in San Francisco. CEO and co-founder Ambuj Kumar joined renowned cryptography expert Benjamin Jun, CEO of HVF Labs, and Docker Security Lead David Lawrence in a session that described how Runtime Encryption and Intel SGX keep a container encrypted during runtime to protect data in use from host OS, root users and network intruders, even if the infrastructure is compromised.

Fortanix was one of 10 finalists for the 2018 RSA Conference Innovation Sandbox Contest for Runtime Encryption. Also, they participated with Intel discussing and showcasing demos of Fortanix Runtime Encryption solutions leveraging Intel SGX at the Intel booth. Those visiting the booth were able to watch a demo to learn about innovations in cloud security that can help organizations securely adopt the cloud even for sensitive workloads or to unlock new value for sensitive data assets.

Finally, Fortanix joined Equinix to discuss Equinix SmartKey, powered by Fortanix, in the Equinix booth, and conducted immersive demos. SmartKey is a global key management and encryption Software as a Service (SaaS) offering that simplifies data protection across any cloud or destination.



1-in-4 orgs using public cloud has had data stolen

McAfee has polled 1,400 IT professionals across a broad set of countries (and continents), industries, and organization sizes and has concluded that lack of adequate visibility and control is the greatest challenge to cloud adoption in an organization. However, the business value of the cloud is so compelling that some organizations are plowing ahead.

According to the survey, 97 percent of worldwide IT professionals are using some type of cloud service. The combination of public and private cloud is the most popular architecture, with 59 percent of respondents now reporting they are using a hybrid model. While private-only usage is relatively similar across all organization sizes, hybrid usage grows steadily with organization size, from 54 percent in organizations up to 1,000 employees, to 65 percent in larger enterprises with more than 5,000 employees.

Top tech firms pledge not to help governments launch cyberattacks

The Cybersecurity Tech Accord is a watershed agreement among the largest-ever group of companies agreeing to defend all customers everywhere from malicious attacks by cybercriminal enterprises and nation-states.

The 34 companies include ABB, Arm, Avast, Bitdefender, BT, CA Technologies, Cisco, Cloudflare, Datastax, Dell, DocuSign, Facebook, Fastly, FireEye, F-Secure, GitHub, GuardTime, HP Inc, HPE, Intuit, Juniper Networks, LinkedIn, Microsoft, Nielsen, Nokia, Oracle, RSA, SAP, Stripe, Symantec, Telefonica, Tenable, TrendMicro, and VMWare.

> The devastating attacks from the past year demonstrate that cybersecurity is not just about what any single company can do but also about what we can all do together. This tech sector accord will help us take a principled path towards more effective steps to work together and defend customers around the world.
> _ Brad Smith, Microsoft President

sensitivity.io

Data Loss Prevention SDK for Cloud, Apps and Services

Advanced scanning, classification and compliance policies by design

www.sensitivity.io

ENDPOINT PROTECTOR

Award-Winning Data Loss Prevention for Windows, macOS and Linux

Ensure compliance, keep data secure and protect all endpoints with refined granular control

www.endpointprotector.com

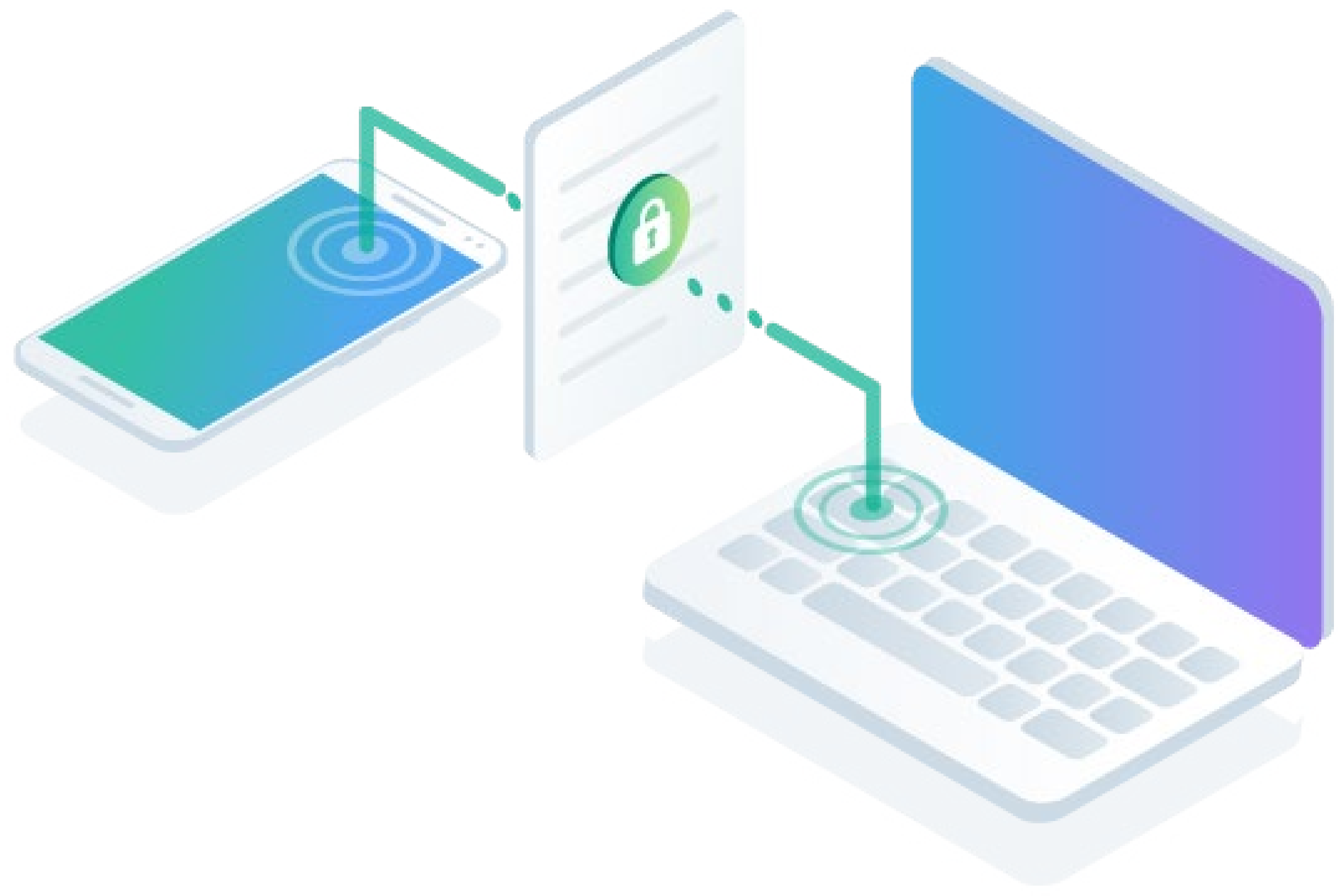
Protect and manage secure company files with Vera's agentless solution

Vera is taking the next step to a truly agentless experience by giving customers the ability to edit, collaborate, and save changes to secure files without requiring any downloads whatsoever.

This new browser-based editing experience makes it easy for enterprises to collaborate on all Office file types — notes, documents, presentations, and more — while preserving the company's policy, security, and control, no matter where the file travels or who has access.

Since its launch in 2015, Vera has always offered the enterprise an agentless security experience. However, to deliver a secure, seamless experience, Vera still required a lightweight agent to facilitate editing documents.

Now, Vera-protected files can be created, shared, accessed, and controlled from any device without the requirement to install an agent, enable fragile plugins, or register new accounts. By eliminating this last hurdle to secure end-to-end collaboration through the last mile, Vera's agentless editing will rapidly spread the adoption of data-centric security across the enterprise.



When we started Vera, we looked at why certain solutions in the market fail. The common theme came down to friction, a bad user experience. With every click you add, there is drop-off and a level of frustration from the user. From enterprise standpoint, the last thing users want to do is install another agent on their device. Today we unveiled the first, most comprehensive rights management solution the world has ever seen. This is where agentless wins.
_ Prakash Linga, CTO and co-founder of Vera

CIO/CISO Interchange launches to discuss security standards

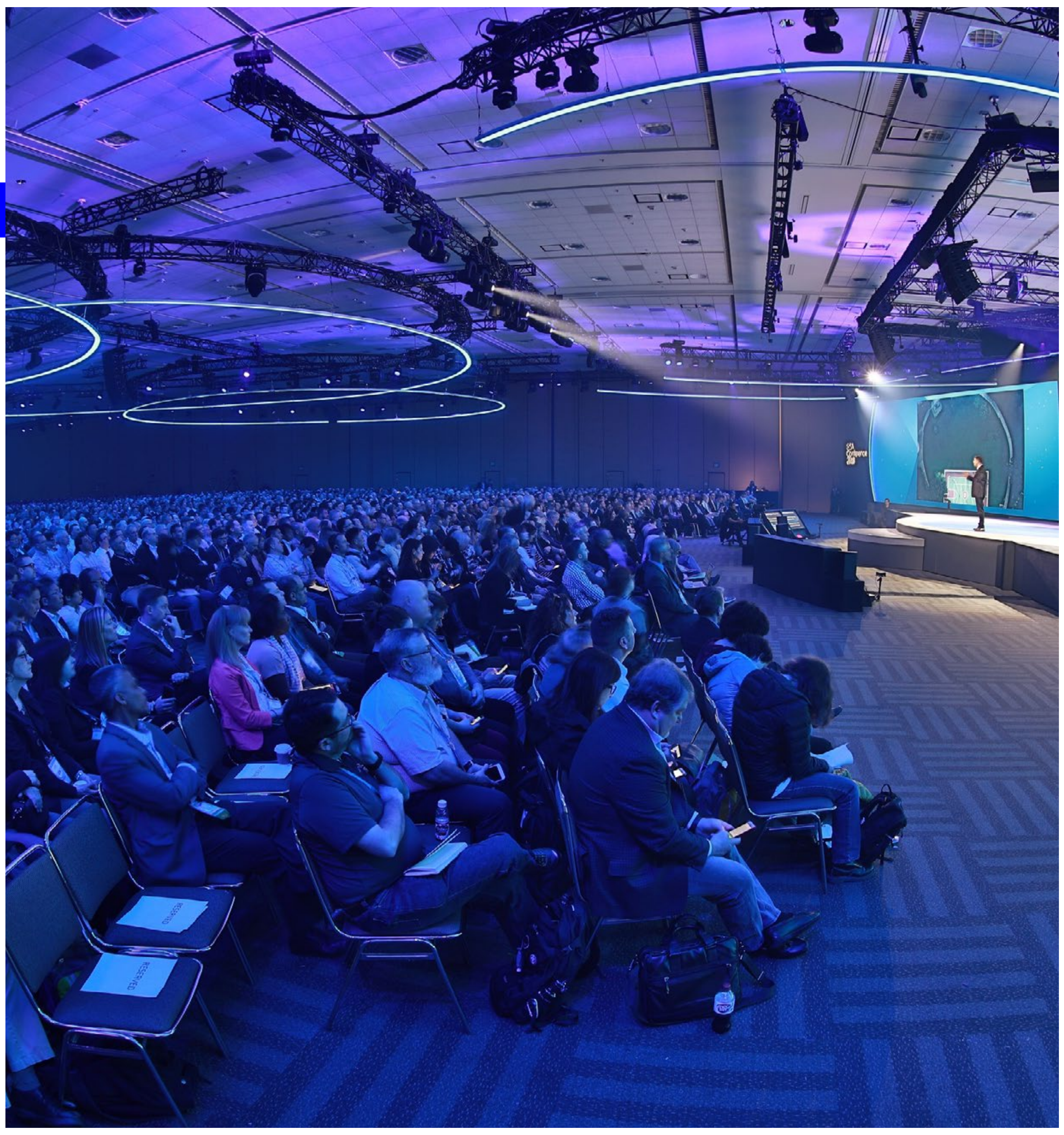
CIO/CISO Interchange, a new non-profit, non-commercial organization co-founded by Philippe Courtot, Chairman & CEO, Qualys, and the Cloud Security Alliance (CSA) was launched during RSA Conference 2018.

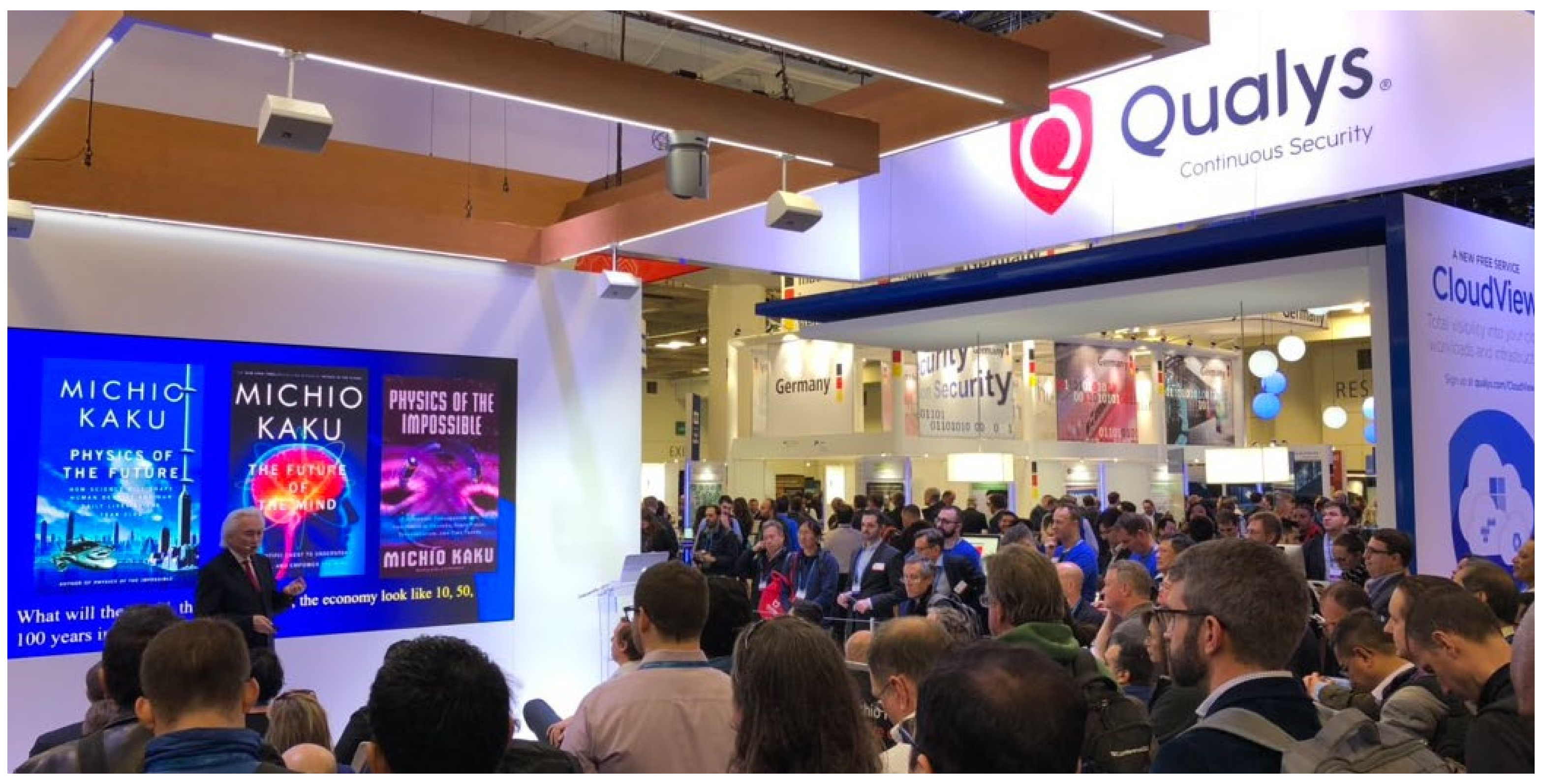
The CIO/CISO Interchange is a private, invitation-only forum for discussions, debates and exchanges between CIOs, CTOs, CISOs and security experts centered around securing the digital transformation. There are no product pitches and no sales personnel, just frank talk on important security issues to help CXOs secure the digital transformation.

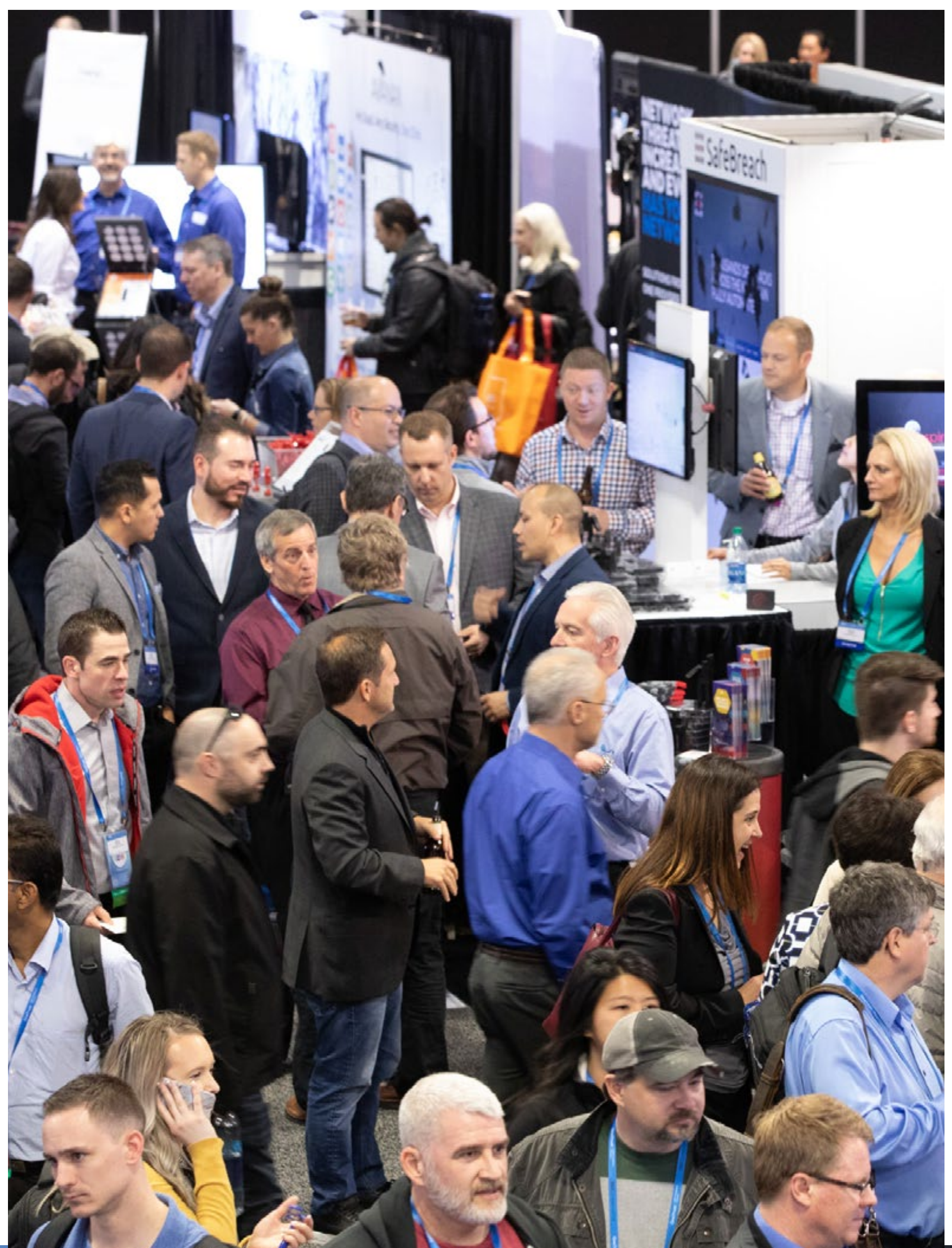
As a co-founding member, Cloud Security Alliance and its community of cloud and security executives will provide the CIO/CISO Interchange with vendor-neutral content and standards for securing the next generation of information technology.

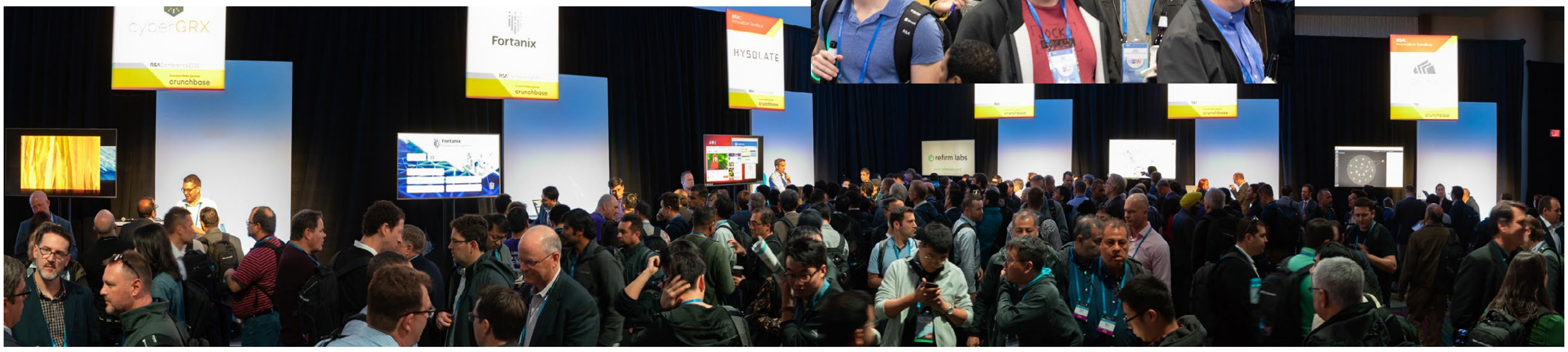
CIO/CISO Interchange's inaugural event took place on Monday, April 16, and the attendees heard a number of speakers, including Philippe Courtot, Julie Ask, VP and principal analyst at Forrester, and noted physicist and futurist Dr. Michio Kaku.

#RSAC 2018 gallery







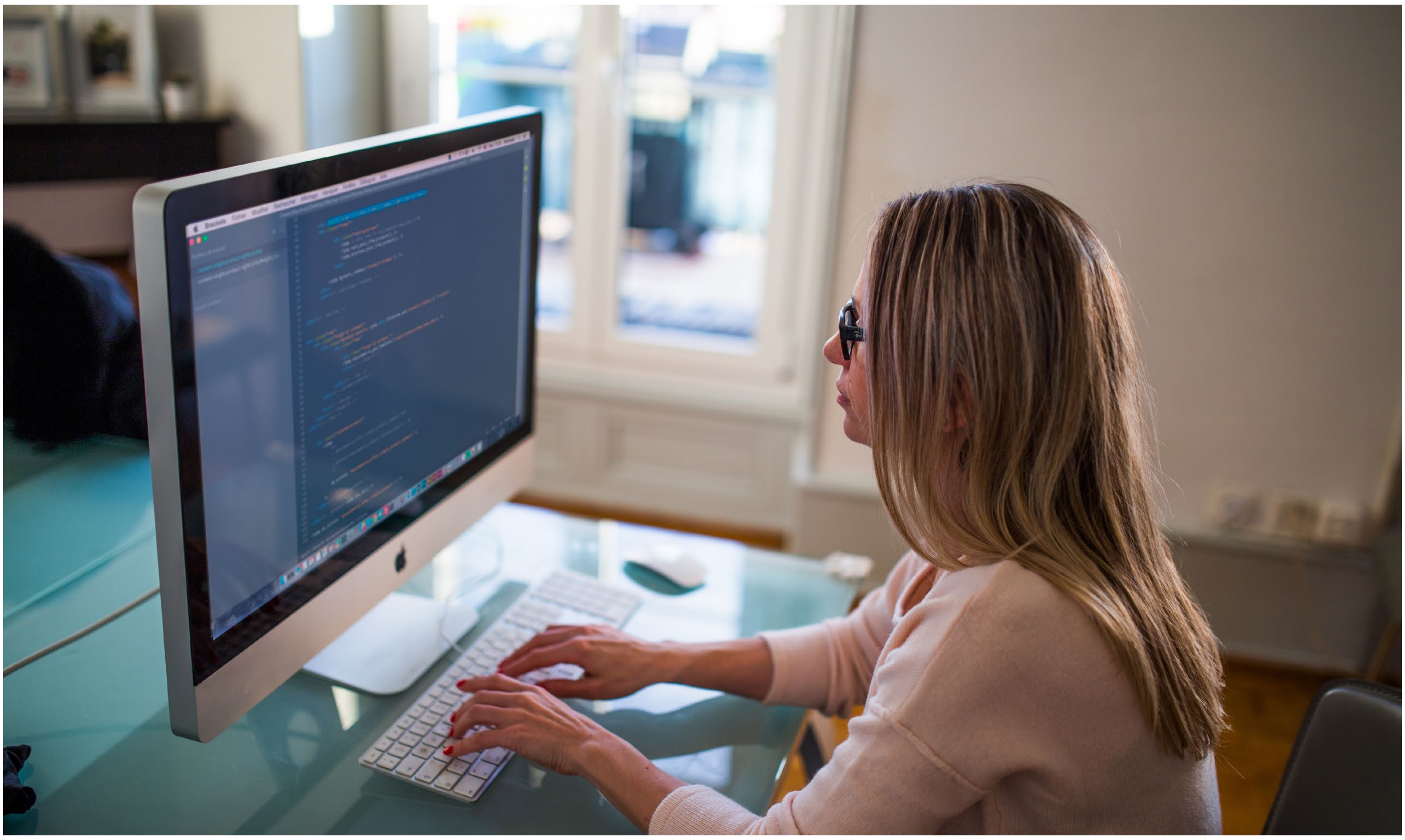


Tech-skilled cybersecurity pros in high demand and short supply

The worldwide cybersecurity skills gap continues to present a significant challenge, with 59 percent of information security professionals reporting unfilled cyber/information security positions within their organization, according to ISACA's new cybersecurity workforce research.

Among the concerning trends:

- High likelihood of cyberattack continues. Four in five security professionals (81 percent) surveyed indicated that their enterprise is likely or very likely to experience a cyberattack this year, while 50 percent of respondents indicate that their organization has already experienced an increase in attacks over the previous 12 months.
- Nearly 1 in 3 organizations (31 percent) say their board has not adequately prioritized enterprise security.
- Men tend to think women have equal career advancement in security, while women say that's not the case. A 31-point perception gap exists between male and female respondents, with 82 percent of male respondents saying men and women are offered the same opportunities for career advancement in cybersecurity, compared to just 51 percent of female respondents. Of those surveyed, about half (51 percent) of respondents report having diversity programs in place to support women cybersecurity professionals.
- Individual contributors with strong technical skills continue to be in high demand and short supply. More than 7 in 10 respondents say their organizations are seeking this kind of candidate.



NIST releases Cybersecurity Framework 1.1

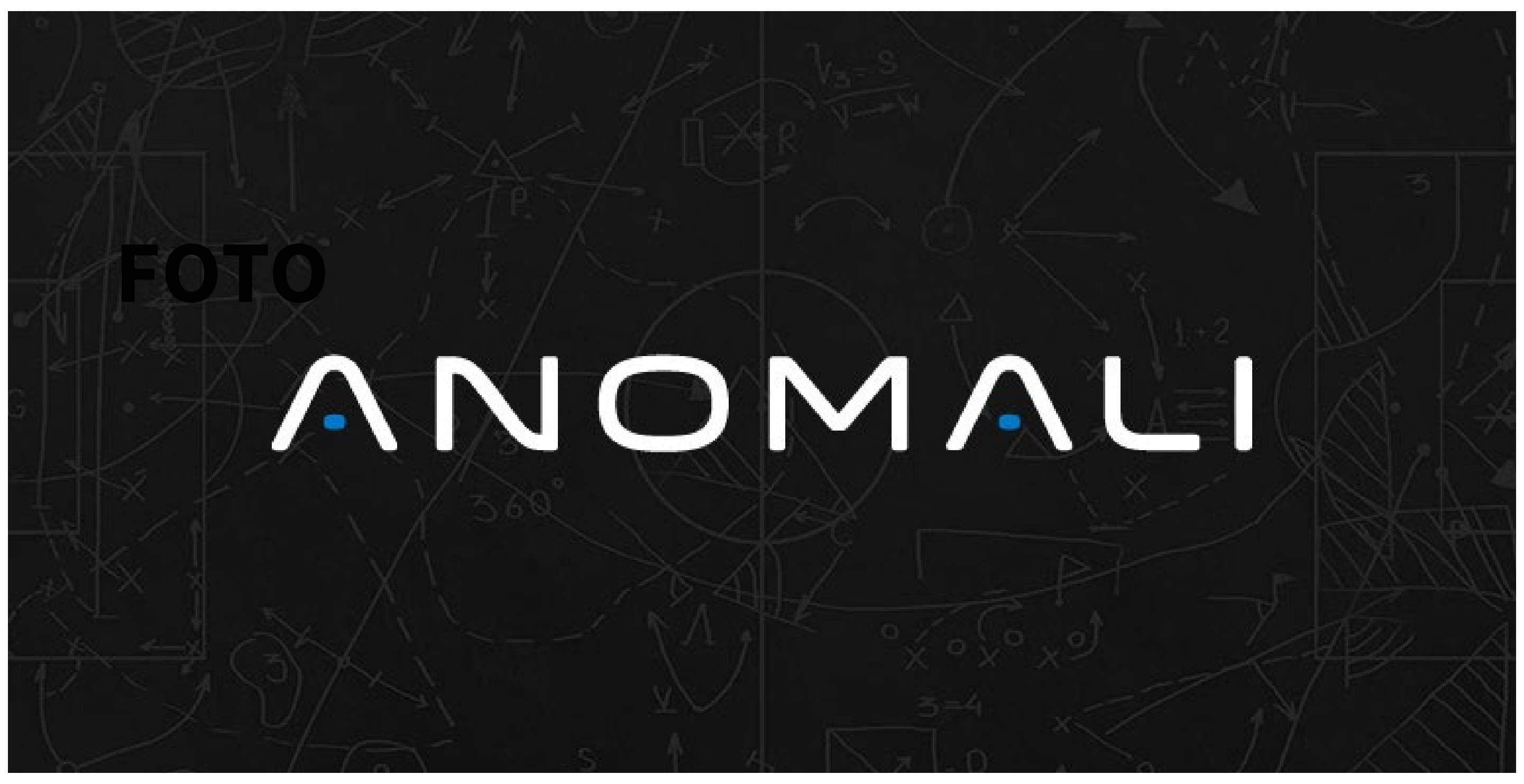
The US Commerce Department's National Institute of Standards and Technology (NIST) released version 1.1 of its popular Framework for Improving Critical Infrastructure Cybersecurity, more widely known as the Cybersecurity Framework.

The changes to the framework are based on feedback collected through public calls for comments, questions received by team members, and workshops held in 2016 and 2017. Two drafts of Version 1.1 were circulated for public comment to assist NIST in comprehensively addressing stakeholder inputs.

> This update refines, clarifies and enhances Version 1.0. It is still flexible to meet an individual organization's business or mission needs, and applies to a wide range of technology environments such as information technology, industrial control systems and the Internet of Things.
> _ Matt Barrett, program manager for the Cybersecurity Framework

Version 1.1 includes updates on:

- Authentication and identity
- Self-assessing cybersecurity risk
- Managing cybersecurity within the supply chain
- Vulnerability disclosure.



Anomali collaborates with Microsoft to integrate threat data

Anomali announced a collaboration with Microsoft to integrate threat intelligence from the Anomali ThreatStream platform with the security insights customers can obtain from the new Microsoft Graph security API.

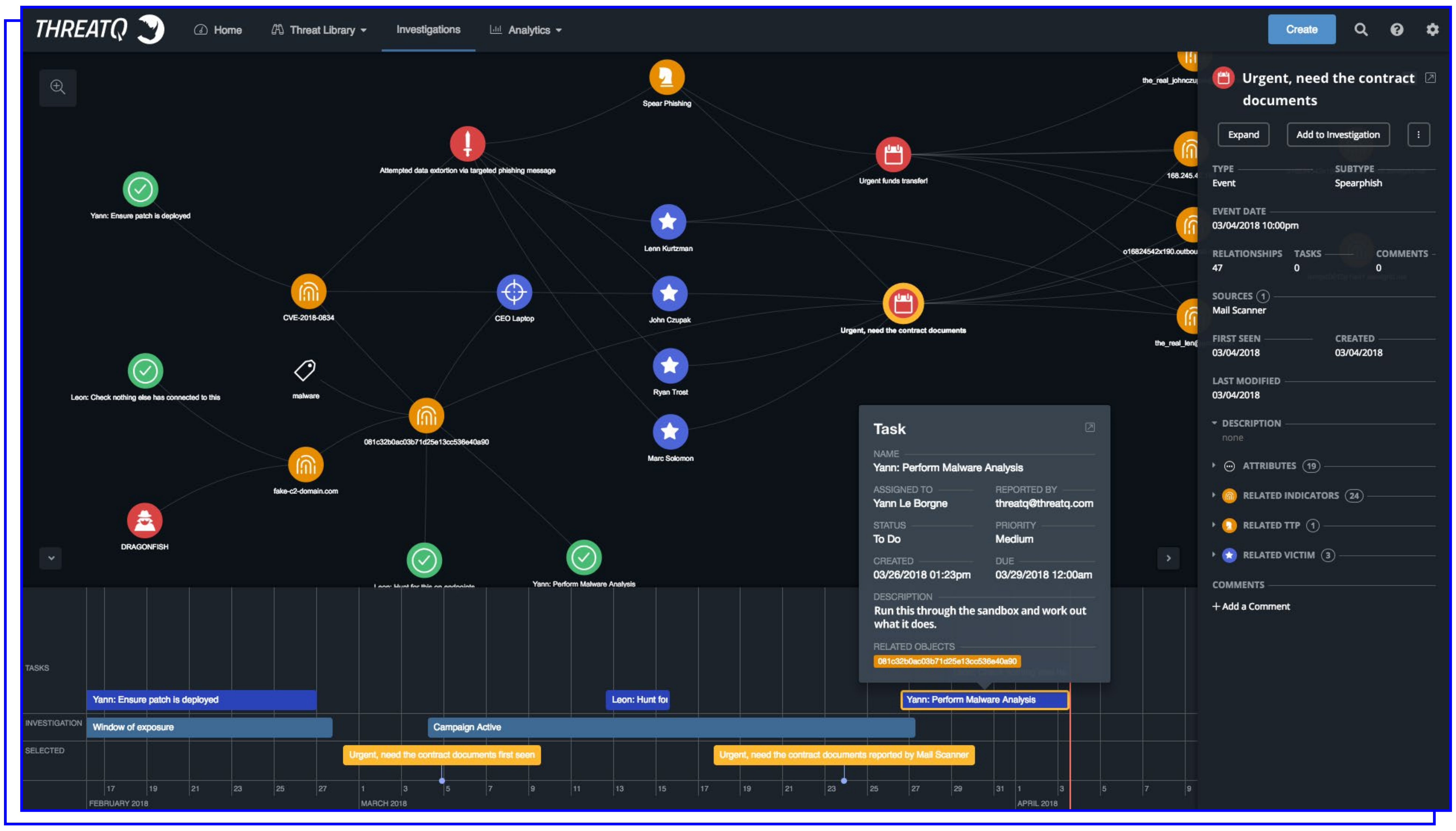
The collaboration provides Microsoft and Anomali customers with the ability to correlate cloud service and network activity with adversary threat information. As the work progresses, the integration will provide a complete view of asset and user information from Graph providers allowing for increased time to detection and more relevant and actionable results.

With contextual and historical threat information provided by Anomali, users have access to not only a detailed background, but also logs of current activity of known IoCs and the malicious actors associated with them.

#RSAC 2018 gallery

ENTERPRISE SOFTWARE-DEFINED WAN
EASY SD-WAN PROVISIONING WITH INTEL AND AT&T
Load balancing and optimized WAN performance
Automated and secure service provisioning
AT&T

ThreatQ Investigations: Cybersecurity situation room accelerates security operations



Task

NAME
Yann: Perform Malware Analysis

ASSIGNED TO
Yann Le Borgne

REPORTED BY
threatq@threatq.com

STATUS
To Do

PRIORITY
Medium

CREATED
03/26/2018 01:23pm

DUE
03/29/2018 12:00am

DESCRIPTION
Run this through the sandbox and work out what it does.

RELATED OBJECTS
081c32b0ac03b71d25e13cc536e40a90

Urgent, need the contract documents

Expand | Add to Investigation

TYPE
Event

SUBTYPE
Spearphish

EVENT DATE
03/04/2018 10:00pm

RELATIONSHIPS
47

TASKS
0

COMMENTS
0

SOURCES (1)
Mail Scanner

FIRST SEEN
03/04/2018

CREATED
03/04/2018

LAST MODIFIED
03/04/2018

DESCRIPTION
none

ATTRIBUTES (19)

RELATED INDICATORS (24)

RELATED TTP (1)

RELATED VICTIM (3)

COMMENTS
+ Add a Comment

ThreatQuotient launched ThreatQ Investigations, a cybersecurity situation room designed for collaborative threat analysis, shared understanding and coordinated response.

ThreatQ Investigations allows real-time visualization of an investigation as it unfolds within a shared environment, enabling teams to better understand and anticipate threats, as well as coordinate a response.

The solution, built on top of the ThreatQ threat intelligence platform, brings order to the chaos of security operations that occurs when teams work in silos, acting independently, inefficiently and unable to share intelligence and tasks easily.

+

With different analysts and teams all working on parallel tasks, it is not uncommon to overlook key commonalities that exist. With ThreatQ Investigations, everyone taking part in an investigation is automatically able to see how the actions of others impact and further extend their own work. ThreatQ Investigations fuses together threat data, evidence, users and actions into a single, shared environment. This unique interface drives collaboration between all parties involved in the investigation process.
_ Leon Ward, VP of Product Management, ThreatQuotient.

Anomali partners with Visa to offer global payment breach intelligence

Threat management and collaboration solutions provider Anomali announced a partnership with Visa to provide cyber security teams with intelligence on indicators of compromise (IoCs) drawn from Visa Threat Intelligence, to better detect and manage breaches involving payment information in retail, hospitality, restaurant and other sectors.

Delivered to the Anomali platform through an API from the Visa Developer Platform, Visa Threat Intelligence enables merchants to collaborate within and across sectors to proactively mitigate threats and work to secure critical access points to protect payment card and personally identifiable information.

Fortanix®

Self-Defending Key Management Service (SDKMS™)

Security + Simplicity

HSM-grade security with Software-defined simplicity

MULTI-CLOUD KEY MANAGEMENT

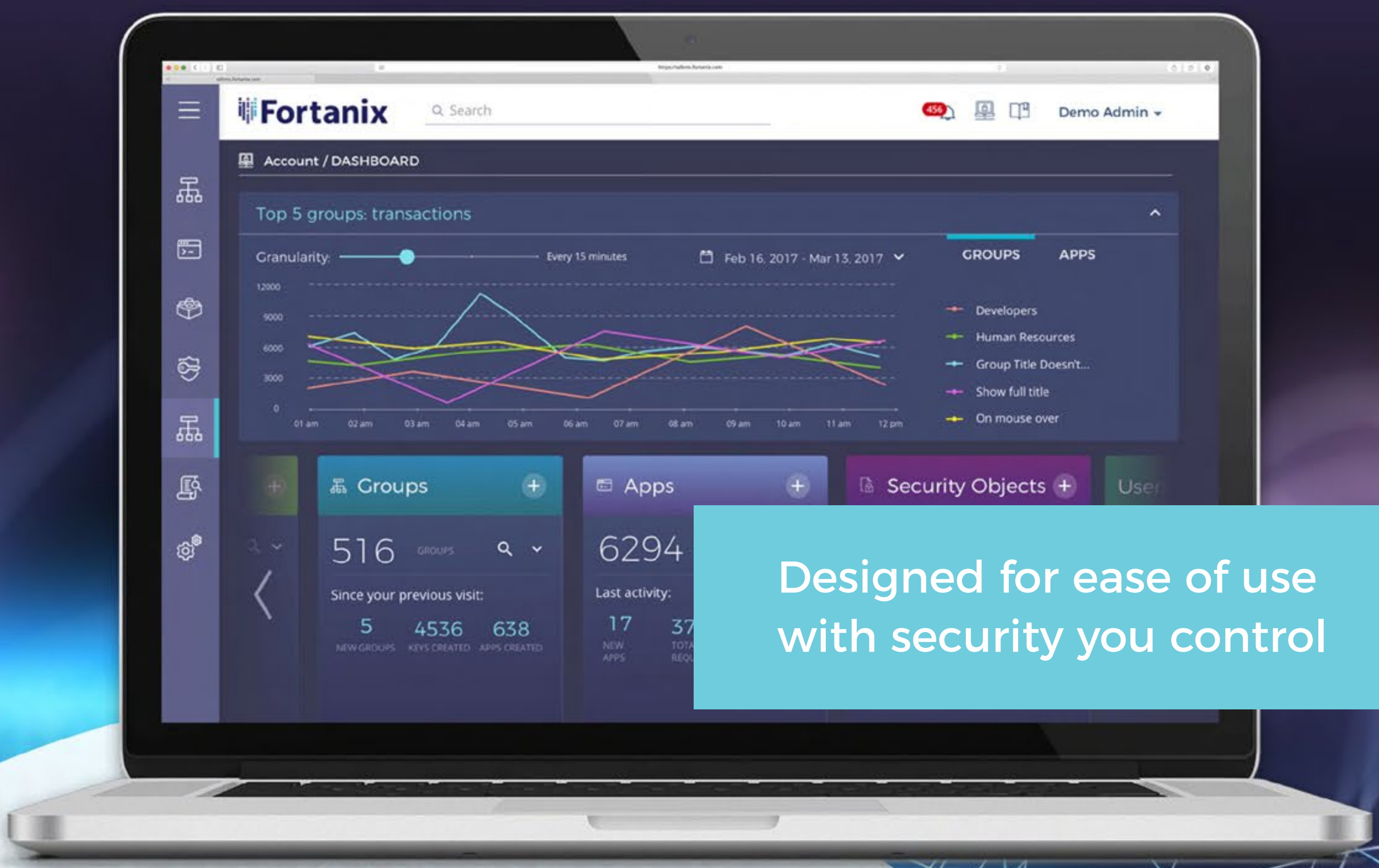
SDKMS enables you to make a secure and seamless transition to hybrid or multi-cloud.
With unified HSM and Key Management capabilities and a scalable distributed architecture, SDKMS can service encryption for any application in any cloud.

Designed for ease of use with security you control

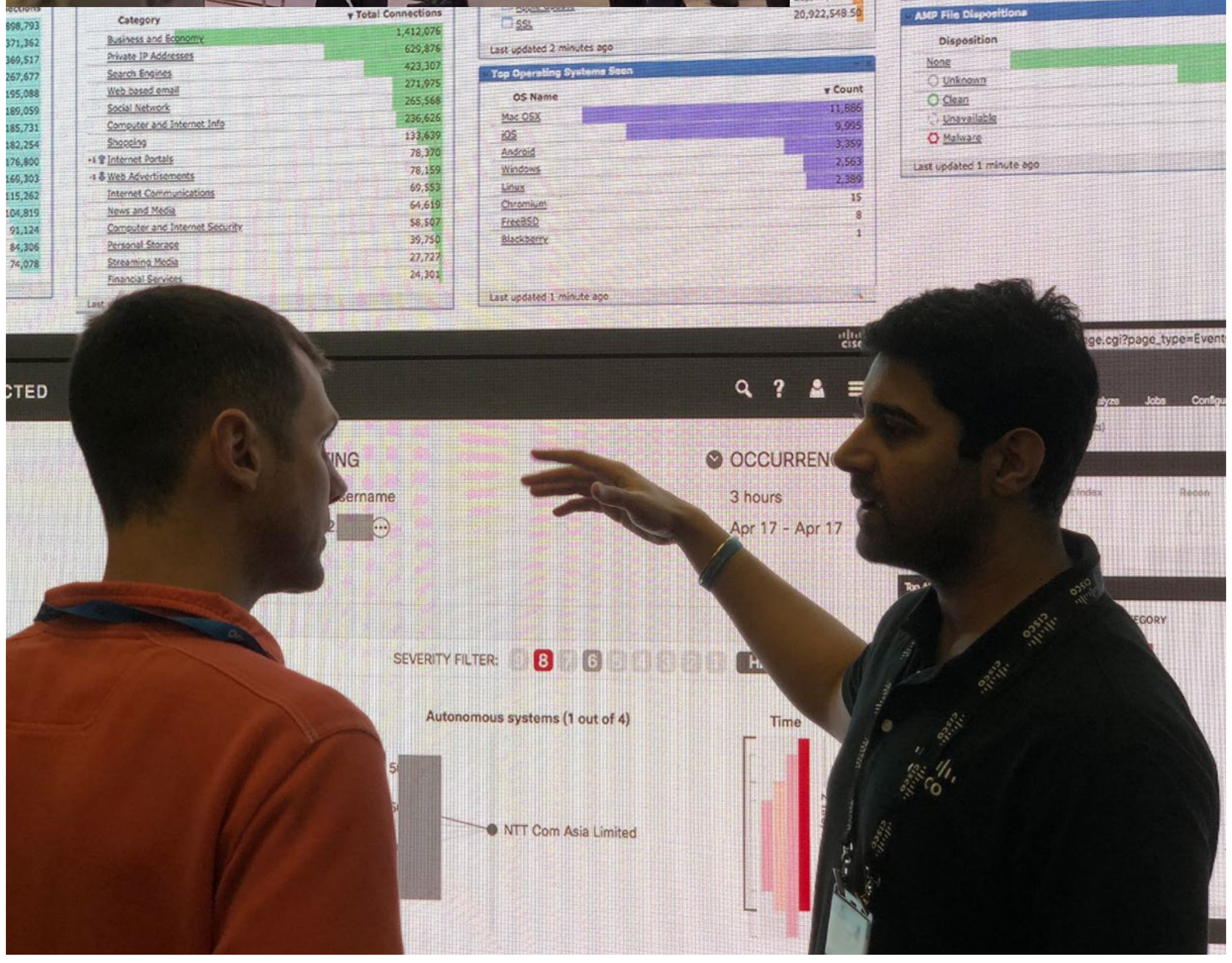
amazon webservices
Microsoft Azure
Google Cloud Platform

linkedin.com/company/fortanix/
facebook.com/fortanix/ @fortanix

www.fortanix.com Leader in Runtime Encryption



#RSAC 2018 gallery



NEHEMIAH SECURITY
Learn more at nehemiahsecurity.com
Align your **security and business** leaders ...
with cyber risk metrics ...
quantified in **dollars and cents**.
Potential Loss to Sales
$300K
$9M
Probability
Severity
Projected Loss
$7.6

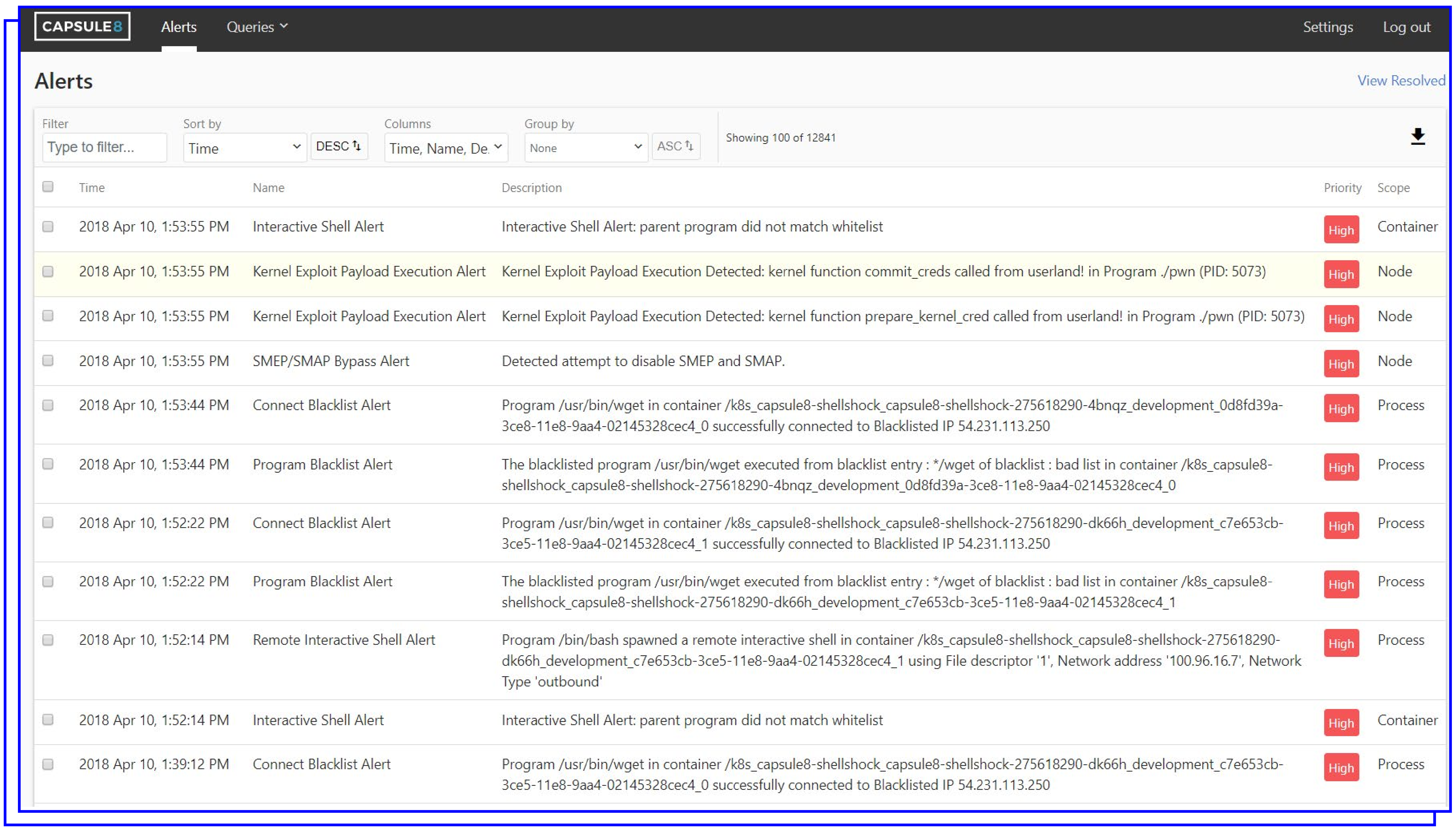
Cisco announces new endpoint and email security services

Nearly all endpoint security solutions on the market claim to block 99 percent of malware. But what about the one percent of threats that evade detection using sophisticated techniques? Cisco Advanced Malware Protection for Endpoints, a cloud-managed endpoint security solution, prevents attacks and helps uncover the one percent of threats that can cripple a business.

Rambus launches fully programmable secure processing core

Rambus announced the availability of the CryptoManager Root of Trust (CMRT), a fully programmable hardware security core built with a custom RISC-V CPU. The secure processing core creates a siloed architecture that isolates and secures the execution of sensitive code, processes and algorithms from the primary processor.

Capsule8 introduces Linux workload attack detection platform



Alerts

Filter: Type to filter...
Sort by: Time DESC
Columns: Time, Name, De.
Group by: None ASC
Showing 100 of 12841

□	Time	Name	Description	Priority	Scope
□	2018 Apr 10, 1:53:55 PM	Interactive Shell Alert	Interactive Shell Alert: parent program did not match whitelist	High	Container
□	2018 Apr 10, 1:53:55 PM	Kernel Exploit Payload Execution Alert	Kernel Exploit Payload Execution Detected: kernel function commit_creds called from userland! in Program ./pwn (PID: 5073)	High	Node
□	2018 Apr 10, 1:53:55 PM	Kernel Exploit Payload Execution Alert	Kernel Exploit Payload Execution Detected: kernel function prepare_kernel_cred called from userland! in Program ./pwn (PID: 5073)	High	Node
□	2018 Apr 10, 1:53:55 PM	SMEP/SMAP Bypass Alert	Detected attempt to disable SMEP and SMAP.	High	Node
□	2018 Apr 10, 1:53:44 PM	Connect Blacklist Alert	Program /usr/bin/wget in container /k8s_capsule8-shellshock_capsule8-shellshock-275618290-4bnqz_development_0d8fd39a-3ce8-11e8-9aa4-02145328cec4_0 successfully connected to Blacklisted IP 54.231.113.250	High	Process
□	2018 Apr 10, 1:53:44 PM	Program Blacklist Alert	The blacklisted program /usr/bin/wget executed from blacklist entry : */wget of blacklist : bad list in container /k8s_capsule8-shellshock_capsule8-shellshock-275618290-4bnqz_development_0d8fd39a-3ce8-11e8-9aa4-02145328cec4_0	High	Process
□	2018 Apr 10, 1:52:22 PM	Connect Blacklist Alert	Program /usr/bin/wget in container /k8s_capsule8-shellshock_capsule8-shellshock-275618290-dk66h_development_c7e653cb-3ce5-11e8-9aa4-02145328cec4_1 successfully connected to Blacklisted IP 54.231.113.250	High	Process
□	2018 Apr 10, 1:52:22 PM	Program Blacklist Alert	The blacklisted program /usr/bin/wget executed from blacklist entry : */wget of blacklist : bad list in container /k8s_capsule8-shellshock_capsule8-shellshock-275618290-dk66h_development_c7e653cb-3ce5-11e8-9aa4-02145328cec4_1	High	Process
□	2018 Apr 10, 1:52:14 PM	Remote Interactive Shell Alert	Program /bin/bash spawned a remote interactive shell in container /k8s_capsule8-shellshock_capsule8-shellshock-275618290-dk66h_development_c7e653cb-3ce5-11e8-9aa4-02145328cec4_1 using File descriptor '1', Network address '100.96.16.7', Network Type 'outbound'	High	Process
□	2018 Apr 10, 1:52:14 PM	Interactive Shell Alert	Interactive Shell Alert: parent program did not match whitelist	High	Container
□	2018 Apr 10, 1:39:12 PM	Connect Blacklist Alert	Program /usr/bin/wget in container /k8s_capsule8-shellshock_capsule8-shellshock-275618290-dk66h_development_c7e653cb-3ce5-11e8-9aa4-02145328cec4_0 successfully connected to Blacklisted IP 54.231.113.250	High	Process

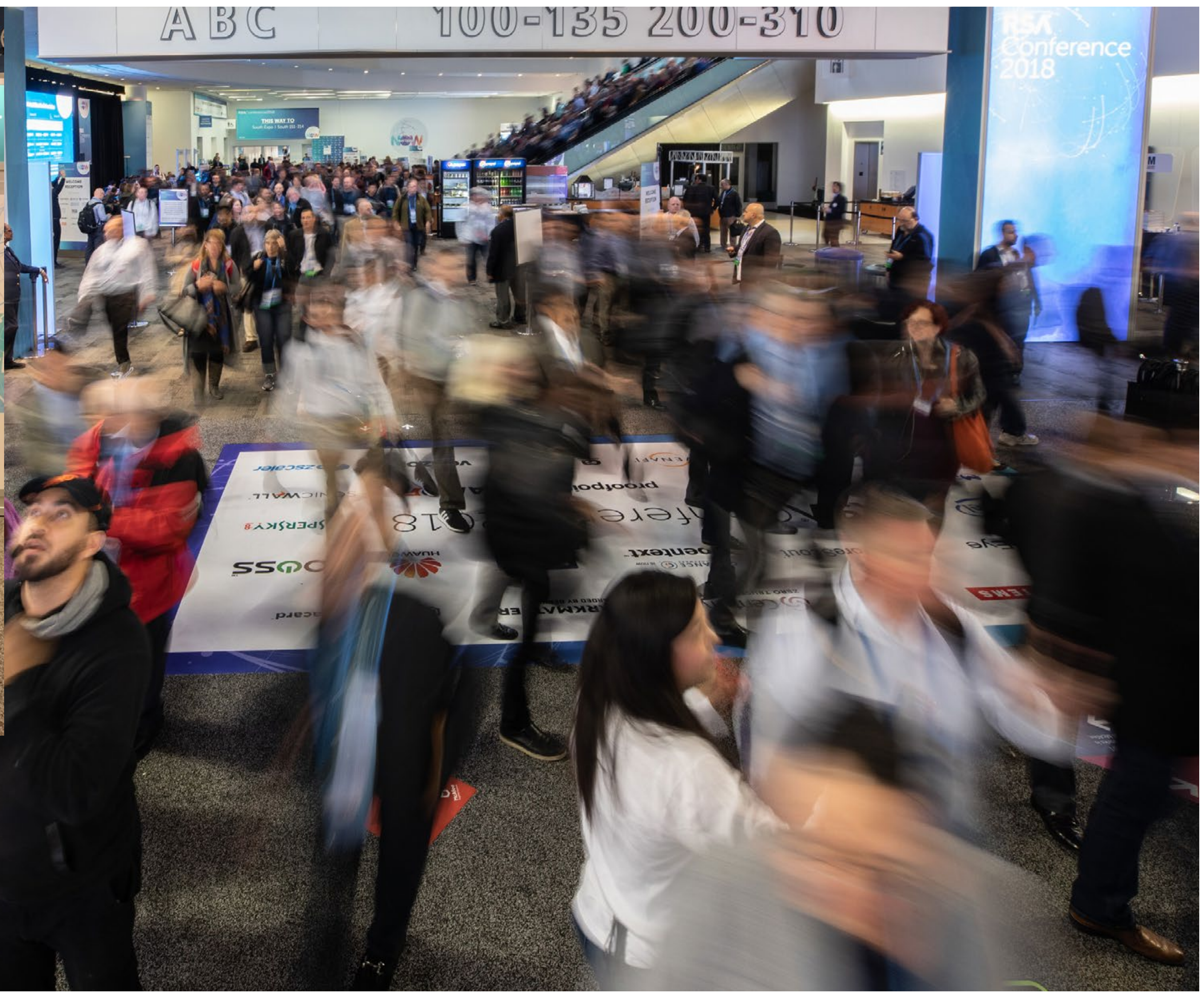
Capsule8 announced the general availability of Capsule8 1.0, a real-time, zero-day attack detection platform capable of scaling to massive production deployments.

As organizations modernize their production infrastructure with technologies like cloud, microservices and containers, they face a changing attack surface that conventional security solutions can't address. And with vulnerabilities such as Meltdown and Spectre, legacy Linux environments such as bare metal and virtual infrastructures are also up against inadequate protection due to low visibility and poor detection. Capsule8 was built to protect today's modern production environment and solve the most critical security challenges associated with both containerized and legacy Linux infrastructures in a single, scalable solution.

> Attack detection is an important focus in microservice environments like Lyft's, where expected host behavior can vary across server fleets. Capsule8's architecture and detection capabilities are impressive and align perfectly with the need for a low-overhead real-time alerting solution which evolves as attackers do. We're glad to see Capsule8 pushing the boundaries of attack detection.
> _ James Addison, senior security engineer at Lyft

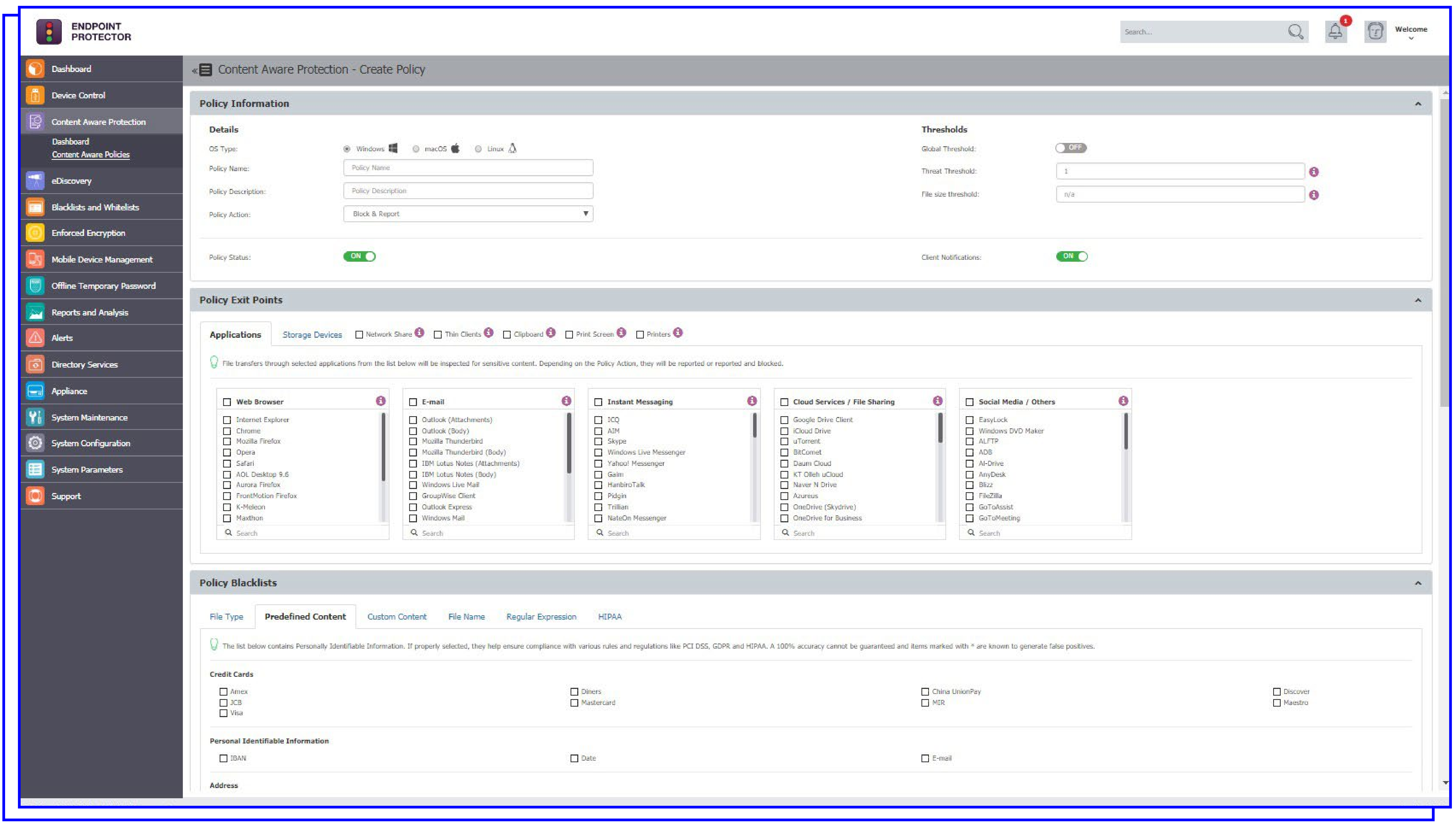
Capsule8 detects and can instantly disrupt attacks in the production environment before the attack takes hold.

#RSAC 2018 gallery



aws
Threat Management
Secure Configuration & Automation
Data Protection & Encryption
aws

In preparation for the GDPR, CoSoSys launches Endpoint Protector 5.1



OS Type: ● Windows ○ macOS ○ Linux
Policy Name: Policy Name
Policy Description: Policy Description
Policy Action: Block & Report
Policy Status: ON
Global Threshold: OFF
Threat Threshold: 1
File size threshold: n/a
Client Notifications: ON

File transfers through selected applications from the list below will be inspected for sensitive content. Depending on the Policy Action, they will be reported or reported and blocked.

The list below contains Personally Identifiable Information. If properly selected, they help ensure compliance with various rules and regulations like PCI DSS, GDPR and HIPAA. A 100% accuracy cannot be guaranteed and items marked with * are known to generate false positives.

CoSoSys announced the latest update of its award-winning flagship Data Loss Prevention product, Endpoint Protector 5.1, which brings added functionalities to key features and a boost for GDPR compliance.

Endpoint Protector 5.1 thus has an extended list of predefined PIIs to cover additional EU countries. Through them, companies can easily track and control data across a larger spectrum.

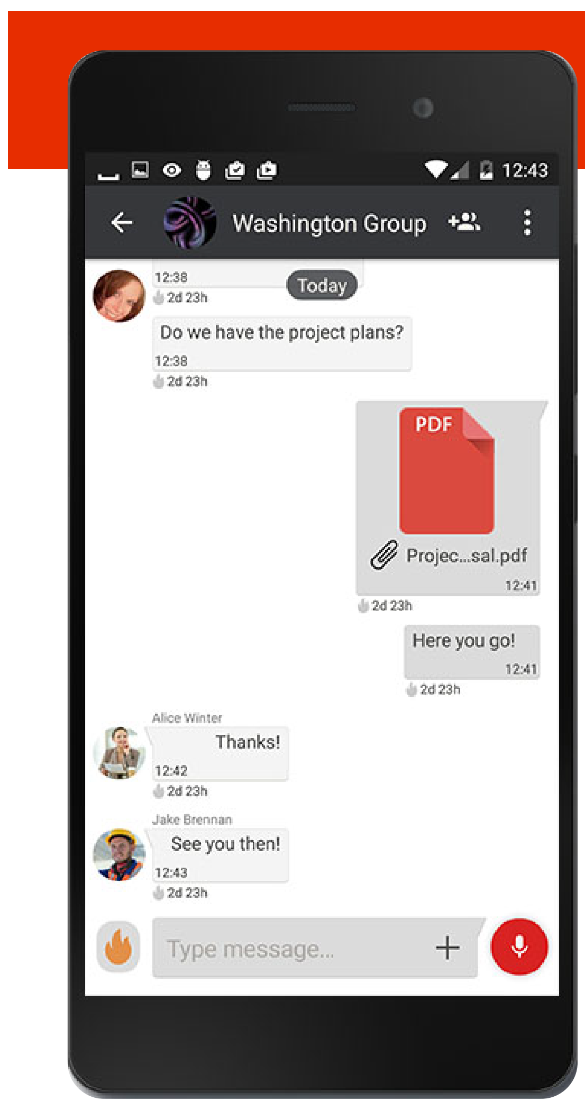
Optical Character Recognition (OCR) has been added so sensitive data can be searched for in images as well. eDiscovery scans, which search data at rest for sensitive information stored on endpoints network-wide and then allow for remediation actions, can now be scheduled to run automatically for a single, one-time scan or for re-occurring scans, on a weekly or monthly basis.

New features include time-based and network-based access rights for computers. While the first allow admins to choose working days and hours and set different access rights according to them, the second defines a company's network through its DNS and ID and grants access rights depending on whether a computer is on them or not.

Another new addition is the Universal Offline Temporary Password which can be used by any user, on any computer, for any device or file transfer, eliminating all security restrictions for one hour. The password can be revoked if there are any security concerns.

Customized IOCs, intelligence and SOC automation

CrowdStrike has expanded the capabilities of the CrowdStrike Falcon platform by introducing a new threat analysis subscription module, CrowdStrike Falcon X. The output of this analysis is a combination of customized indicators of compromise (IOCs) and threat intelligence designed to help prevent against threats your organization faces now and in the future.


Washington Group
Today
Do we have the project plans?
Projec...sal.pdf
Here you go!
Alice Winter
Thanks!
Jake Brennan
See you then!
Type message...

Envelop your Communications in a Silent Circle

Silent Phone brings our enterprise-grade security features to iOS, Android and Silent OS mobile devices. Lock down your communication from end-to-end with the only enterprise messaging app you can control.

GoSilent empowers users with enterprise security in the palm of their hand. Trust employees to go silently with our portable VPN, Firewall built for IoT edge security with government-grade encryption.

silent circle

NOTHING SEEN,
NOTHING HEARD,
NOTHING DISCLOSED.

Onapsis raises $31 million Series C funding for ERP cybersecurity

Onapsis, the global experts in business-critical application cybersecurity and compliance, today announced a $31 million Series C minority funding round led by new investor LLR Partners, with participation from existing institutional investors .406 Ventures, Evolution Equity Partners and Arsenal Venture Partners.

This marks the largest single round of funding in the company's history, bringing the total investment in Onapsis to $62 million. David Stienes, Partner at LLR Partners, will join the company's board of directors.

The expanded investment in Onapsis will help further accelerate the company's growth and position as the leader in protecting ERP systems and business-critical applications, such as SAP and Oracle. These applications run the Global 2000 and manage their crown jewels ranging from sensitive customer and employee information to finances, manufacturing processes and intellectual property, yet they have historically been left exposed and are a perfect economic target for attackers. The potential downtime, data breaches and fraud can result in significant negative financial and reputational impact.

> We are excited to welcome LLR Partners to the Onapsis team, augmenting the group of industry-leading investors who support our vision of securing the world's business-critical applications. The capital investment will be dedicated to fueling growth and delivering even more value to our customers and partners.
> _ Mariano Nunez, CEO and Co-founder of Onapsis

MinerEye introduces AI-powered Data Tracker

MinerEye is launching MinerEye Data Tracker, an AI-powered governance and data protection solution that will enable companies to continuously identify, organize, track and protect vast information assets including undermanaged, unstructured and dark data for safe and compliant cloud migration.

Infrastructure-agnostic web app protection with virtual patching option

Signal Sciences announced the latest innovations for its Web Protection Platform. Its patented architecture provides security, operations and development teams with the visibility, security and scalability needed to protect against the full spectrum of threats their web applications now face, from OWASP Top 10 to account takeovers, API misuse and bots.

Passwordless enterprise authentication on Windows 10 and Azure AD

Yubico announced that the new Security Key by Yubico supporting FIDO2 will be supported in Windows 10 devices and Microsoft Azure Active Directory (Azure AD). The feature is currently in limited preview for Microsoft Technology Adoption Program (TAP) customers.

The only Threat Intelligence Platform designed to
ACCELERATE SECURITY OPERATIONS
Now with the industry's first cybersecurity situation room, ThreatQ™ Investigations.
ThreatQ.com/investigations
THREATQUOTIENT™

ONLY VERA PROTECTS:

☑ FILES
☑ EMAIL
☑ BOX
☑ DROPBOX
☑ OFFICE 365
☑ ALL YOUR DATA

Secure confidential data with a single click. Track every access to data, anywhere it goes. Dynamically change permissions, add watermarks, and instantly revoke access. Take back control of your data with Vera.

To learn more, visit vera.com

VERA

Third-party and insider threats one of the biggest concerns to IT pros

External threats are not the main concern for IT professionals, but rather breaches that are linked to vulnerabilities caused by staff or third-party vendors operating within an organization's own network, Bomgar's 2018 Privileged Access Threat Report reveals.

In fact, 50% of organizations claimed to have suffered a serious information security breach or expect to do so in the next six months, due to third-party and insider threats – up from 42% in 2017. Additionally, 66% of organizations claimed that they could have experienced a breach due to third-party access in the last 12 months, and 62% due to insider credentials.

However, a large part of this risk sits with the organizations themselves, as the report found that 73% rely on third-party vendors too heavily, and 72% have cultures that are too trusting of partners.

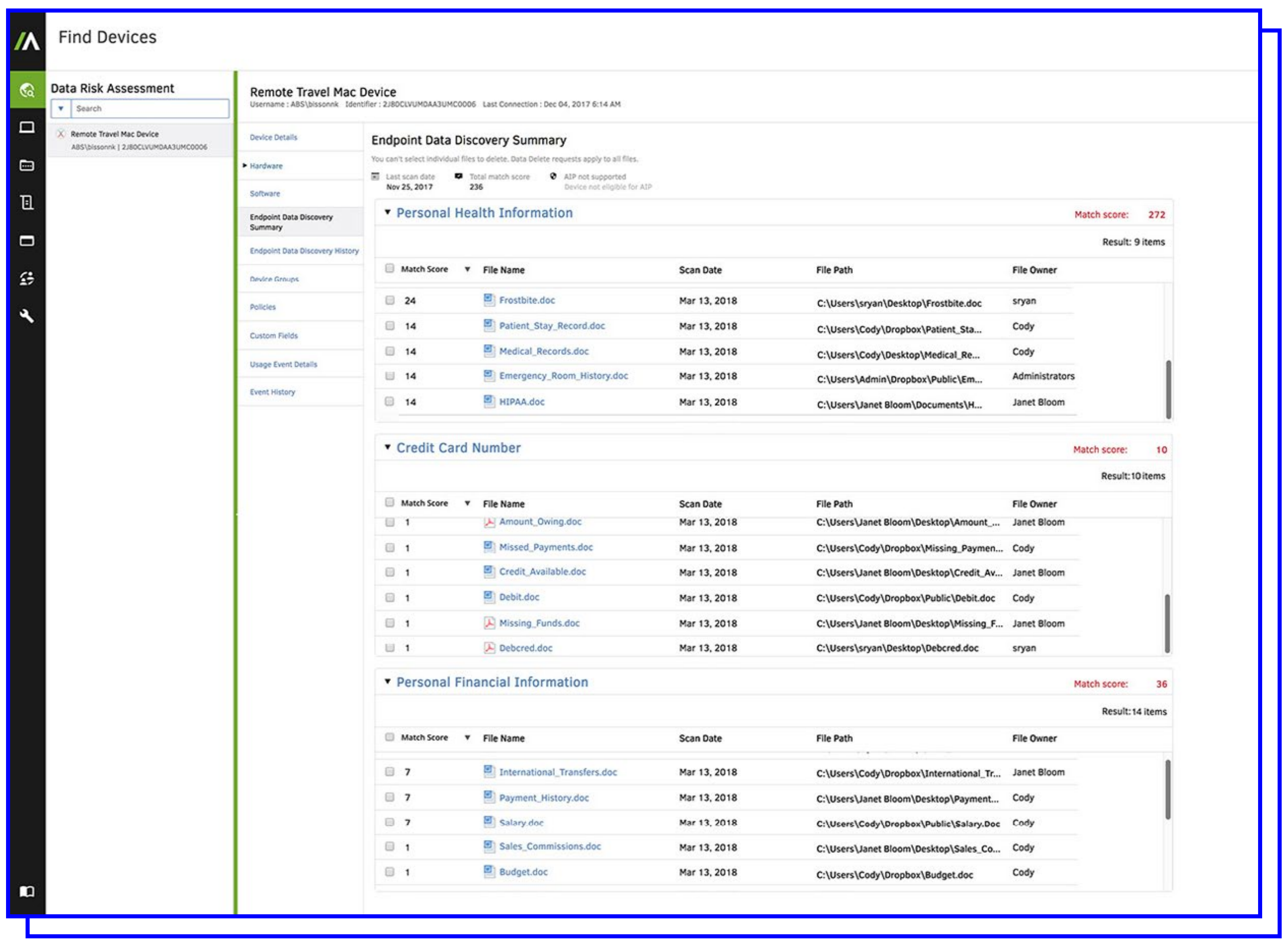
Absolute debuts GDPR data risk assessment

Absolute announced new GDPR Data Risk and Endpoint Readiness Assessments to accelerate compliance with the impending GDPR. Absolute's new assessments offer deep insights and actionable recommendations to better protect and manage endpoints, where sensitive data might be accessed, stored or shared.

Increasingly sophisticated security incidents and escalating regulatory demands are placing unprecedented pressure on IT security to maintain constant visibility and control over data and endpoints. Dark endpoints and the sensitive data residing on them present significant dangers, especially as the enforcement of GDPR looms.

With more and more regulations on the horizon, it is essential that organizations be able to identify, monitor and remediate all endpoints, even those outside of the network. Absolute's robust readiness assessment is an important first step to jump-start GDPR corporate compliance, especially when ensuring endpoint visibility and device usage across on-premises, cloud and mobile networks. The assessments leverage the power of Absolute's platform and embedded Persistence technology to provide a complete understanding of the status of every endpoint, including those that have gone dark.

> Enterprises struggle under immense security and regulatory pressures as a result of today's global digital environments. With Absolute's GDPR Data Risk and Endpoint Readiness Assessments, we provide companies with a universal place to begin their compliance journey by quickly identifying areas of concern, and more importantly, actionable ways to address them. By leveraging the powerful Absolute platform for assessment, organizations will gain unprecedented visibility into the complex web of their endpoints and data residing on them, in order to swiftly take action and promptly meet compliance requirements such as GDPR.
> _ Chris Covell, CIO at Absolute



Remote Travel Mac Device
ABS\bissonnk | 2J8OCLVUMDAA3UMC0006

Remote Travel Mac Device
Username : ABS\bissonnk Identifier : 2J8OCLVUMDAA3UMC0006 Last Connection : Dec 04, 2017 6:14 AM

Endpoint Data Discovery Summary

You can't select individual files to delete. Data Delete requests apply to all files.

Last scan date Nov 25, 2017 | Total match score 236 | AIP not supported Device not eligible for AIP

Personal Health Information — Match score: 272

Result: 9 items

□ Match Score	File Name	Scan Date	File Path	File Owner
□ 24	Frostbite.doc	Mar 13, 2018	C:\Users\sryan\Desktop\Frostbite.doc	sryan
□ 14	Patient_Stay_Record.doc	Mar 13, 2018	C:\Users\Cody\Dropbox\Patient_Sta...	Cody
□ 14	Medical_Records.doc	Mar 13, 2018	C:\Users\Cody\Desktop\Medical_Re...	Cody
□ 14	Emergency_Room_History.doc	Mar 13, 2018	C:\Users\Admin\Dropbox\Public\Em...	Administrators
□ 14	HIPAA.doc	Mar 13, 2018	C:\Users\Janet Bloom\Documents\H...	Janet Bloom

Credit Card Number — Match score: 10

Result: 10 items

□ Match Score	File Name	Scan Date	File Path	File Owner
□ 1	Amount_Owing.doc	Mar 13, 2018	C:\Users\Janet Bloom\Desktop\Amount_...	Janet Bloom
□ 1	Missed_Payments.doc	Mar 13, 2018	C:\Users\Cody\Dropbox\Missing_Paymen...	Cody
□ 1	Credit_Available.doc	Mar 13, 2018	C:\Users\Janet Bloom\Desktop\Credit_Av...	Janet Bloom
□ 1	Debit.doc	Mar 13, 2018	C:\Users\Cody\Dropbox\Public\Debit.doc	Cody
□ 1	Missing_Funds.doc	Mar 13, 2018	C:\Users\Janet Bloom\Desktop\Missing_F...	Janet Bloom
□ 1	Debcred.doc	Mar 13, 2018	C:\Users\sryan\Desktop\Debcred.doc	sryan

Personal Financial Information — Match score: 36

Result: 14 items

□ Match Score	File Name	Scan Date	File Path	File Owner
□ 7	International_Transfers.doc	Mar 13, 2018	C:\Users\Cody\Dropbox\International_Tr...	Janet Bloom
□ 7	Payment_History.doc	Mar 13, 2018	C:\Users\Janet Bloom\Desktop\Payment...	Cody
□ 7	Salary.doc	Mar 13, 2018	C:\Users\Cody\Dropbox\Public\Salary.Doc	Cody
□ 1	Sales_Commissions.doc	Mar 13, 2018	C:\Users\Janet Bloom\Desktop\Sales_Co...	Cody
□ 1	Budget.doc	Mar 13, 2018	C:\Users\Cody\Dropbox\Budget.doc	Cody

BigID is this year's most innovative startup at RSA Conference

BigID was named "Most Innovative Startup" at the 2018 RSA Conference Innovation Sandbox Contest.

A judging panel comprised of venture capitalists, entrepreneurs and industry veterans selected BigID from a group of 10 finalists and announced the winner at RSA Conference 2018.

Based in New York and Tel Aviv, BigID uses advanced machine learning and identity intelligence to help enterprises better protect their customer and employee data at petabyte scale. Using BigID, enterprises can better safeguard and assure the privacy of their most sensitive data, reducing breach risk and enabling compliance with emerging data protection regulations like the EU GDPR.

"We're honored to have been considered against this group of fantastic companies and thrilled to accept this award," said Dimitri Sirota, CEO of BigID. "We believe that privacy is a defining 21st century problem that all companies are going to have to take seriously and our hope is that we can help make it less painful for them."

Fortanix was recognized as well by judges for Runtime Encryption.

Devs know application security is important, but have no time for it

Sonatype polled 2,076 IT professionals to discover practitioner perspectives on evolving DevSecOps practices, shifting investments, and changing perceptions, and the results of the survey showed that breaches related to open source components grew at a staggering 50% since 2017, and 121% since 2014.

This follows on from Sonatype's findings earlier in the year, which showed that 1 in 8 open source components downloaded by developers in the UK contained a known security vulnerability.

Yet despite this, resourcing and training still presents challenges: 48% of respondents admitted that they don't have enough time to spend on application security, while 35% of developers from companies with no DevOps practices received no training on application security in the past year.

Distributed security event correlation solution helps SOCs combat cyber-attacks

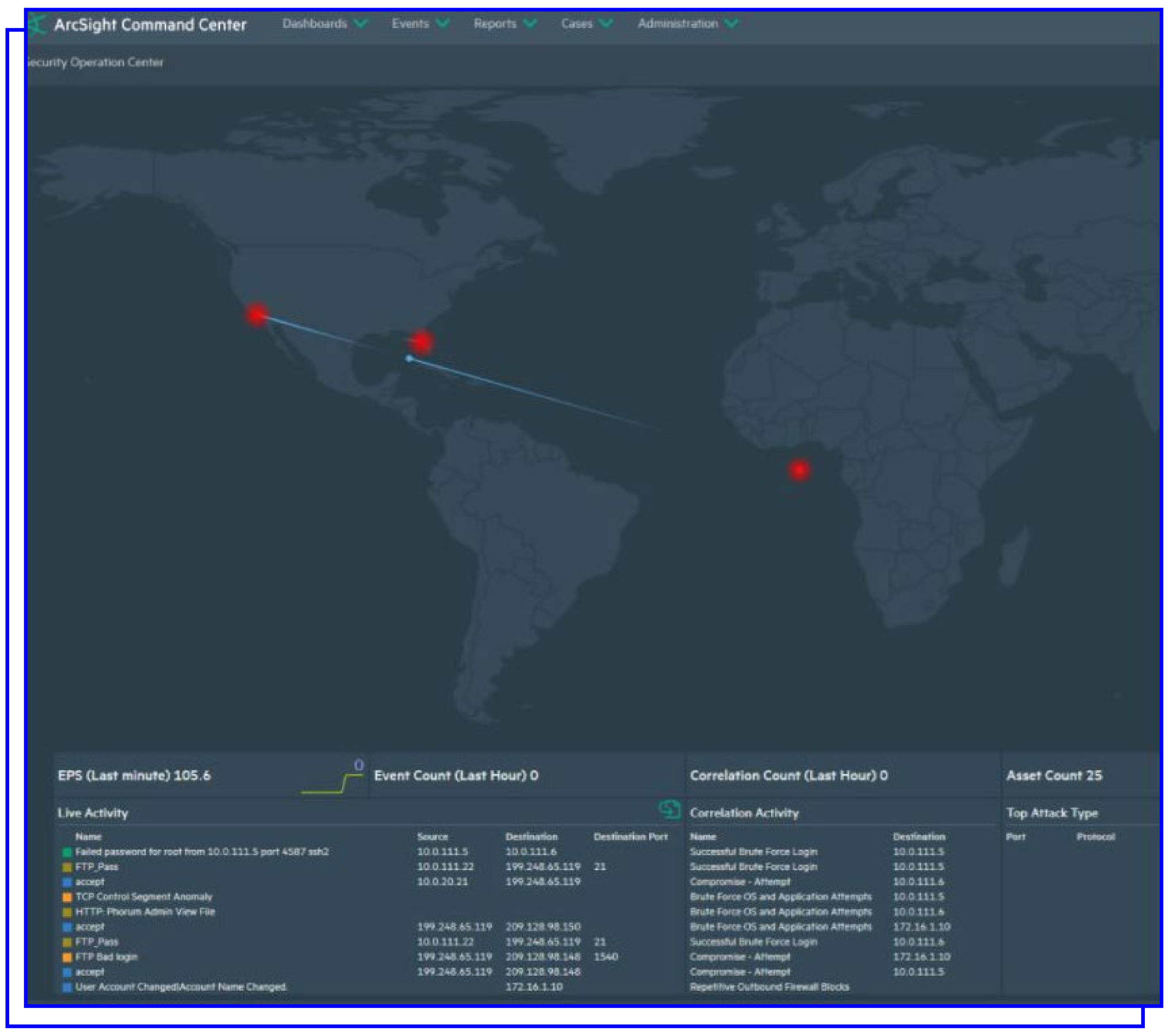
Micro Focus announced ArcSight Enterprise Security Manager (ESM) 7.0, the latest release of its solution that prioritizes security threats and compliance violations with real-time threat intelligence to quickly identify and impede potential cyber-attacks.

Micro Focus ArcSight ESM 7.0 enables security operations centers (SOCs) to become agile, expand their cyber security footprint and respond quickly to evolving threats.

By collecting, correlating, and reporting security event information at a massive scale (up to 100,000 correlated events per second, per cluster) it helps organizations meet even the most demanding security requirements, while simplifying and improving time to value.

With ArcSight ESM 7.0 and its newly introduced distributed correlation, customers will find:

- Improved correlation fidelity with more contextual event analysis
- More efficient use of resources as ESM dynamically identifies EOI
- Improvements to ESM availability and redundancy
- Better cost/performance flexibility
- Flexible expansion and capacity planning options to solve for a wider set of security use cases
- Backwards compatibility with existing rules & content
- The ability to get more value from existing security tools and events.



EPS (Last minute) 105.6

Event Count (Last Hour) 0

Correlation Count (Last Hour) 0

Asset Count 25

Live Activity

	Name	Source	Destination	Destination Port
🟩	Failed password for root from 10.0.111.5 port 4587 ssh2	10.0.111.5	10.0.111.6	
🟨	FTP_Pass	10.0.111.22	199.248.65.119	21
🟦	accept	10.0.20.21	199.248.65.119	
🟧	TCP Control Segment Anomaly			
🟨	HTTP: Phorum Admin View File			
🟦	accept	199.248.65.119	209.128.98.150	
🟨	FTP_Pass	10.0.111.22	199.248.65.119	21
🟧	FTP Bad login	199.248.65.119	209.128.98.148	1540
🟦	accept	199.248.65.119	209.128.98.148	
🟦	User Account Changed|Account Name Changed.		172.16.1.10	

Correlation Activity

Name	Destination
Successful Brute Force Login	10.0.111.5
Successful Brute Force Login	10.0.111.5
Compromise - Attempt	10.0.111.6
Brute Force OS and Application Attempts	10.0.111.5
Brute Force OS and Application Attempts	10.0.111.6
Brute Force OS and Application Attempts	172.16.1.10
Successful Brute Force Login	10.0.111.6
Compromise - Attempt	172.16.1.10
Compromise - Attempt	10.0.111.5
Repetitive Outbound Firewall Blocks	

Top Attack Type

Port	Protocol