



#RSAC

2017

ISSUE 52.5

SAN FRANCISCO EDITION

FEBRUARY 2017

CONNECT  
TO PROTECT



# GOT 2-SECOND VISIBILITY?

**ACHIEVE 2-SECOND VISIBILITY** across your on-premise, endpoint and elastic cloud global IT assets.

**CONTINUOUSLY ASSESS** your security and compliance posture, and identify whether you've been compromised.

**DRASTICALLY REDUCE YOUR TCO** by consolidating multiple enterprise security and compliance solutions with the Qualys Cloud Platform – *and more to come.*



Sign up for a free trial at  
[qualys.com/2seconds](https://qualys.com/2seconds)

A record number of more than 43,000 attendees experienced keynotes, peer-to-peer sessions, track sessions, tutorials and seminars at the 26th annual RSA Conference in San Francisco in February.

UnifyID was named "RSA Conference 2017's Most Innovative Startup" by the Innovation Sandbox's judges' panel comprised of technology, venture and security industry thought leaders.

43,000  
attendees

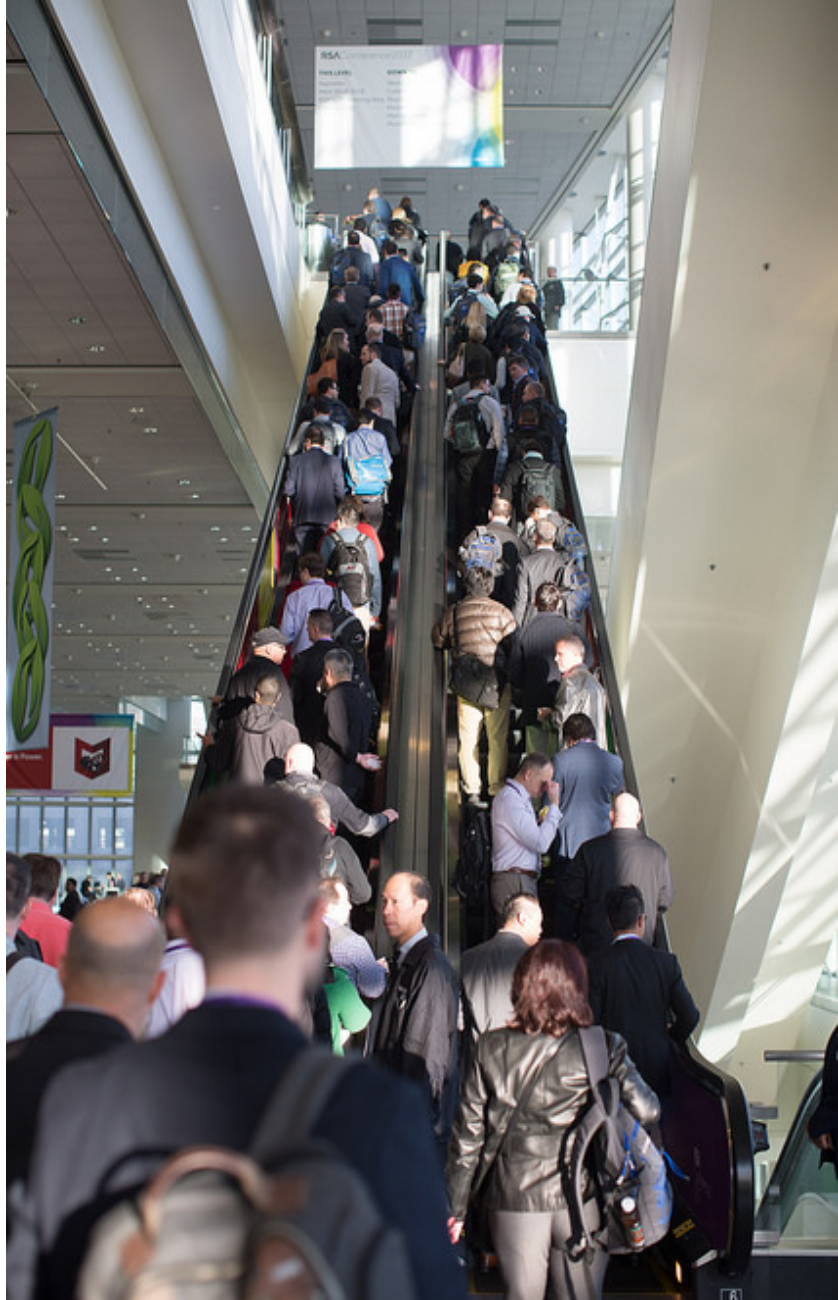
RSA Conference reached broader audiences with a new series of educational programs that teaches cyber-awareness for children, provides outreach to college students to introduce and encourage a career in information security, and supports education throughout the various stages of a career within the industry.

RSA Conference created College Day to help students find their ideal career options through meeting both industry veterans and companies that are looking for young, talented students to join their ranks.

This year 60 students had access to more than 50 sessions, a day in the life of a security expert panel, and met with sponsors during an open house that was attended by more than 600 attendees.

This year's winners of the RSA Conference Awards included:

- Howard Schmidt, Former White House Cybersecurity Advisor – Excellence in the Field of Information Security
- Dr. Tatsuaki Okamoto, NTT Fellow – Excellence in the Field of Mathematics
- The Honorable Michael McCaul, Chairman, U.S. House of Representatives, Homeland Security Committee – Excellence in the Field of Public Policy.



"Leading up to RSA Conference 2017 it could have been argued that this event was the most anticipated in our history," said Linda Gray Martin, Director & General Manager of RSA Conference. "Over the last few months information security has experienced both tremendous highs, and weathered scrutiny of lows as experts in private and public sectors debated various practices of information sharing. As a result of this increased exposure, it was critical to have an RSA Conference full of constructive dialog, discussion and debate that will form the information security agenda and continue to move our industry forward. We hope our attendees took this powerful opportunity as the chance to help forge a future we can all be proud of."



# Sponsors of our coverage from RSA Conference 2017

## DIAMOND SPONSOR



## PLATINUM SPONSORS



## GOLD SPONSORS



cybereason



NTT Security



iovation®



THREATQUOTIENT



Skycure  
Mobile Threat Defense



TOPSPIN  
SECURITY

VERA

## SILVER SPONSORS



Absolute - 8, 24

AlienVault - 23, 34

Bitglass - 6, 23

Cybereason - 12, 23, 28

DigiCert - 32

Dome9 - 23

Easy Solutions - 8, 28

InfoArmor - 8, 12

iovation - 34

Qualys - 16, 17, 18, 19, 20, 21, 23, 32

Ntrepid - 32

NTT Security - 8

ThreatQuotient - 24, 32

TopSpin Security - 32

Vera - 24, 32

## (IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - [mzorz@helpnetsecurity.com](mailto:mzorz@helpnetsecurity.com)

News: Zeljka Zorz, Managing Editor - [zzorz@helpnetsecurity.com](mailto:zzorz@helpnetsecurity.com)

Marketing: Berislav Kucan, Director of Operations - [bkucan@helpnetsecurity.com](mailto:bkucan@helpnetsecurity.com)

Photography by RSA Conference and (IN)SECURE Magazine.

Distribution: (IN)SECURE Magazine can be freely distributed in the form of the original, non-modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor.





**See a  
real attack**  
on a virtual  
network.

[go.nehemiahsecurity.com/real-attack](https://go.nehemiahsecurity.com/real-attack)

# PRODUCT SPOTLIGHT

## Bitglass announces integration with Trustwave Managed Security Services

Bitglass announced new integration with the Trustwave Managed Detection service. This service has been enhanced to support events and additional threat intelligence from leading cloud access security broker (CASB) providers like Bitglass. This increased security visibility helps Trustwave detect cloud-based threats earlier by leveraging support for the latest CASB technologies.



As enterprises adopt cloud and mobile, visibility and control of corporate data outside the firewall becomes a critical component of a complete security strategy. Paired with Bitglass' CASB solution, organizations can now deploy the Trustwave Managed Detection service for intelligent, actionable alerts and analysis that incorporates data from cloud and mobile security events.

## Trustwave introduces proactive threat hunting service

Trustwave announced new and enhanced managed security and professional services designed to help short-circuit an attacker's activities by detecting cybersecurity threats much earlier and shutting them down before real damage is done.

## Intel Security's strategy for eliminating cybersecurity fragmentation

At the heart of a unified strategy for cybersecurity is the need for integrated solutions that tie into the enterprise's framework to address top-of-mind challenges. Intel Security announced new and updated solutions that do exactly that: McAfee Enterprise Security Manager (ESM) 10 and McAfee Virtual Network Security Platform (vNSP).

## Logtrust debuts analytics solution for detecting threats in real-time

Logtrust announced its Real-time Integrated Threat Analytics Solution Program. The program enables companies to build solutions that analyze the historical behavior of systems and attackers in order to detect, understand and eliminate potential threats in real-time – even those that are coming from multiple sources, across multiple devices.

## Remote credential rotation for distributed environments

Bomgar introduced Bomgar Vault 17.1, the first enterprise password management solution to offer remote credential rotation from an on-premise solution with its new RotateAnywhere technology.





**THREATQUOTIENT**

# EMPOWER THE HUMAN ELEMENT OF CYBERSECURITY

Strengthen your security posture with a threat intelligence platform designed to enable threat operations and management; and arm your analysts with the intelligence, controls and automation required to protect your business, employees and customers.



2016 WINNER  
CRN EMERGING  
VENDORS LIST



BEST SECURITY  
COMPANY OF THE  
YEAR (SOFTWARE)



STARTUP  
OF THE YEAR



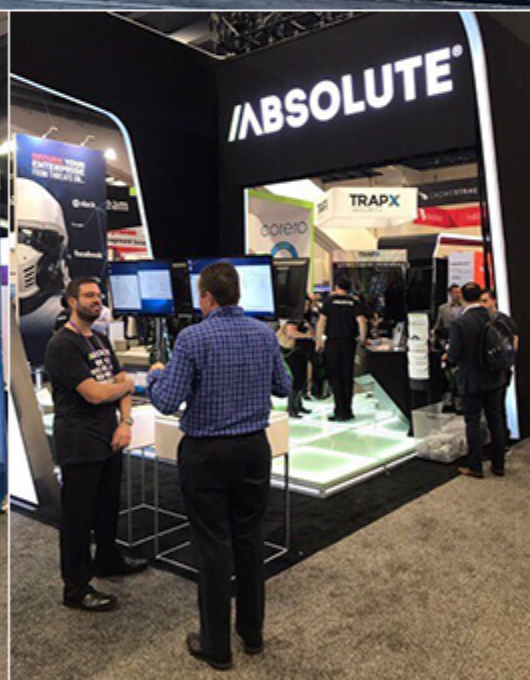
INNOVATION  
IN ENTERPRISE  
SECURITY



SINET 16  
INNOVATOR  
AWARD

**THREATQ.COM**







# DARK ENDPOINTS ARE A BREEDING GROUND FOR SECURITY BREACHES

Get the always-on visibility and real-time remediation you need to stop security breaches at the source. Exclusive, self-healing endpoint security from Absolute.

Absolute sees and secures what others cannot:

- › Eliminate blind spots in endpoints on and off the network
- › Instantly remediate compromised endpoint controls
- › Reduce vulnerabilities caused by user error and attacks
- › Trust the solution already embedded in over one billion devices



Protect your devices, data, applications and users with exclusive, self-healing endpoint security from Absolute. Find out how in your free report: [www.absolute.com/IDCreport](http://www.absolute.com/IDCreport)

**ABSOLUTE™**  
Always There. Already There.



## 25% of web apps still vulnerable to eight of the OWASP Top Ten

69 percent of web applications are plagued by vulnerabilities that could lead to sensitive data exposure, and 55 percent by cross-site request forgery flaws, the results of a security research project on web application vulnerabilities by Contrast Security revealed.

Broken authentication and session management issues affect 41 percent of web apps, while security misconfiguration and lack of function level access control is found on 37 and 33 percent of apps, respectively.

The research also found that 80 percent of tested software applications had at least one vulnerability, with an average of 45 vulnerabilities per application.

These results are based on the data collected from the Contrast Security platform across several popular development languages.

Contrast Labs compared the top web application vulnerabilities across two of the most popular web application development languages: Java and .NET.

In so doing, they revealed that Java suffers from higher prevalence of cross-site request forgery (impacting 69 percent of Java applications, as compared to 31 percent in .NET) and less security misconfiguration problems than .NET (14 percent in Java versus 73 percent in .NET).

This is almost certainly because .NET relies far more on configuration than Java applications do. However, the high numbers of security misconfiguration in .NET indicate that this approach is not without its own set of problems.





Passages

Secure Isolated Browser

# ELIMINATE WEB-DELIVERED MALWARE

[www.Ntrep.id/helpnet](http://www.Ntrep.id/helpnet)

## TOTAL PROTECTION AGAINST:

Browser-Based Malware

Watering Hole Attacks

Spear Phishing

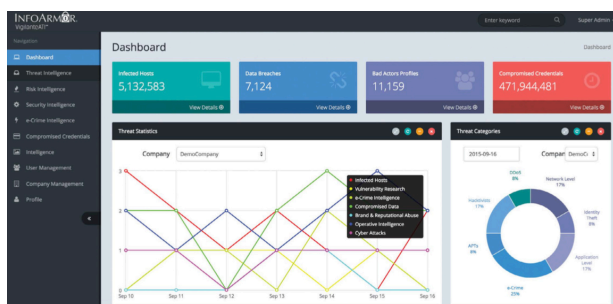
Drive-by Downloads

**N**TREPID®

# PRODUCT SPOTLIGHT

## InfoArmor VigilanteATI: Threat intelligence from the Dark Web

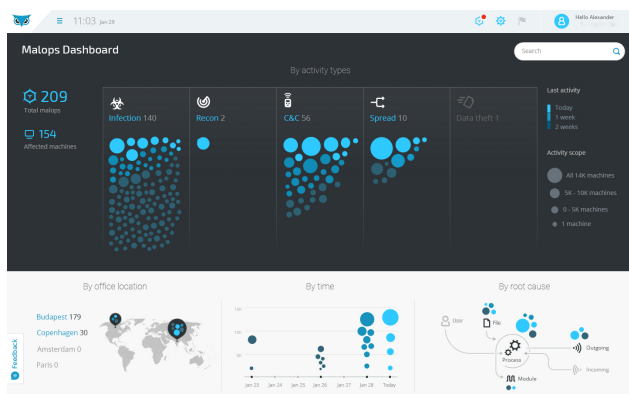
InfoArmor has expanded its customer base in the enterprise and SME/SMB sector with its VigilanteATI Advanced Threat Intelligence Platform and Investigative Services.



From preemptive attacks to post-breach attribution, VigilanteATI helps organizations enhance their security posture.

## Cybereason unveils complete next-generation endpoint platform

Cybereason unveiled a new Endpoint Security Platform that includes next-generation antivirus functionality. By integrating Cybereason's endpoint detection and response platform with classic and next-generation antivirus, enterprises can secure their environment against threats on a single agent for ease of deployment and management.



## IBM Watson to power cognitive security operations centers

Watson for Cyber Security will be integrated into IBM's new Cognitive SOC platform, bringing together advanced cognitive technologies with security operations and providing the ability to respond to threats across endpoint, network, users and cloud.

## Cybrary training management and skills assessment platform

Designed for enterprise users, Cybrary Teams provides access to Cybrary's training catalogue through a customizable in-browser dashboard. There, enterprises can manage its members, export member training data to their learning management system.

## Targeted attack prevention in cloud email and messaging systems

The GreatHorn Threat Platform (GTP) enables organizations to tap into the threat data, machine-learning, and automated response framework that underpins GreatHorn's threat detection and response solutions for social engineering, phishing, and targeted attack prevention in cloud email and messaging systems.

## AI SaaS application for cyber attack detection

PatternEx announced the first Artificial Intelligence SaaS application for cyber attack detection. PatternEx's flagship product, the PatternEx Threat Prediction Platform, is available as a SaaS application with a free trial period to selected customers.



# CAPSULE8

**Modernize without Compromise**

**Container-Aware, Real-Time  
Threat Protection for Linux**

**Learn more about our  
RSA launch and product updates  
[info@Capsule8.io](mailto:info@Capsule8.io)**

**[www.Capsule8.io](http://www.Capsule8.io)**



---

## Half of IT pros lack confidence in their company's cybersecurity strategies

Centrify asked IT professionals attending RSA Conference 2017 how their companies secure applications and infrastructure in the age of access, and their responses revealed that a startling number lacked confidence in their own organization's corporate security.

---

## 26 percent of respondents still share passwords, despite an increase in breaches

---

Only slightly more than half (55%) stated they believe their company's current technology investment ensures their company's cybersecurity. But when asked about which of the 15 different identity and access management (IAM) best practices they use, it turns out that many fall short on implementing enough of them to warrant a confidence score.

Among 15 different IAM best practices, organizations are most likely to enforce:

- Single sign-on (68 percent)
- Adaptive multi-factor authentication (43 percent)
- Least privileged access (44 percent)
- No sharing of privileged accounts (36 percent)
- Secure remote access without a VPN (35 percent).

Organizations are least likely to enforce privileged session recording (13 percent), granular automatic deprovisioning across server and app accounts (12 percent), and privilege elevation management (8 percent).





# 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 revoke access, instantly. Take back control of your data with Vera.

To learn more, visit [vera.com](https://vera.com)

**VERA**



Continuously discover and secure all of your global IT assets

## Qualys brings web application security automation to a new level

Qualys announced new functionality in its web application security offerings, including scalable fast scanning, detection and patching of websites, mobile applications and Application Programming Interfaces (APIs) in one unified platform.

New features in Qualys Web Application Scanning (WAS) 5.0 and Web Application Firewall (WAF) 2.0 allow customers to scan thousands of web applications and APIs using

WAS 5.0, deploy one-click virtual patches for detected vulnerabilities using WAF 2.0 and manage it all from a centralized self-updating cloud platform.

Web application security is complex due to the continuously evolving threat landscape, the diverse nature of web, mobile and Internet of Things (IoT) applications and the broad range of systems needed to manage security across them. Qualys is addressing this complexity by extending automated web application vulnerability scanning to APIs, and adding increased WAF customization capabilities, simplified controls and stronger security rules.

Customers can now use one cloud platform to programmatically scale rapid scanning and patching of web application vulnerabilities across browser-based, mobile and IoT services, then simulate attacks to verify protection.

QUALYS® ENTERPRISE

Web Application Scanning

Dashboard Web Application Scanning

Web Application Scanning

Search Results

Filter Results

Tags

Scan Information

Schedule Information

Scanner Appliance

Scanner Tags

Last Scan Status

Web Application Creation

Step 2 of 11

1 Asset Details

2 Application Details

3 Scan Settings

4 DNS Override

5 Crawl Settings

6 Redundant Links

7 Authentication

8 Crawl Exclusion Lists

9 Malware Monitoring

10 Comments

11 Review And Confirm

Tell us about the web application you want to scan

Target Definition

Web Application URL  
https://api.iotservice.com

Crawl Scope\*

Limit at or below URL hostname (api.iotservice.com)

Scope will be limited to the hostname within the URL: https://api.iotservice.com/, using HTTP or HTTPS and any port. All links discovered on the api.iotservice.com domain will be in scope. For example, all links discovered in https://api.iotservice.com/support/ and https://api.iotservice.com:8080/logout/ will be in scope. Links outside the api.iotservice.com domain are not in scope. This means, for example, links like https://api2.iotservice.com and https://cdn.api.iotservice.com will not be in scope.

Explicit URLs to Crawl / REST Paths and Parameters / SOAP WSDL Location

https://api.iotservice.com/REST/subscriber?=1234567

Cancel Previous Continue

Scanned Updated

06 Feb 2017 06 Feb 2017

13 Jan 2016 03 Jan 2017

13 Dec 2016 13 Dec 2016

22 Oct 2015 05 Feb 2016

19 Dec 2015 19 Dec 2015

23 Nov 2015 16 Dec 2015

Actions View Report

About Terms of Use Support



This agile solution will also empower DevOps teams to make web application security an integral part of their processes, so they can detect and patch vulnerabilities early on in the development cycle, avoiding costly security issues in production.

### **WAS 5.0 offers:**

**Programmatic scanning of SOAP and REST-based APIs** – In addition to scanning Simple Object Access Protocol (SOAP) APIs, Qualys WAS architecture now allows testing of REpresentational State Transfer (REST) API services. Users need only provide the service locations in the Qualys WAS user interface and the scanner will test for common application security flaws.

**IoT and mobile app backend scanning** – With SOAP and REST API scanning capabilities, WAS can now test IOT services and mobile apps as well as API-based business-to-business connectors for security flaws with the precision and scale of the Qualys Cloud Platform.

**Unprecedented scalability with parallelization of scanning resources** – WAS now automatically load-balances scanning of multiple applications across a pool of scanner appliances to complete the scan efficiently. This means less idle time for the scanning appliances, with greater coverage.

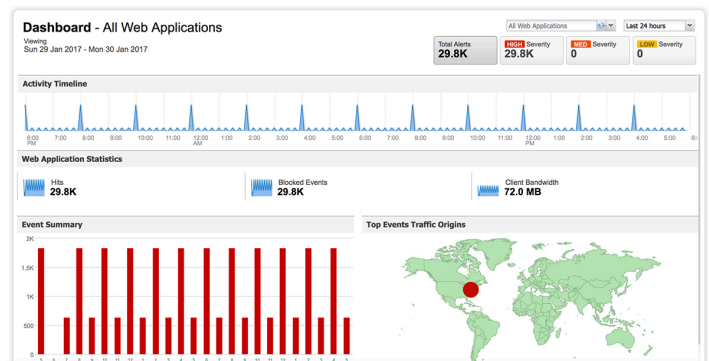
**Increased coverage** – Improvements to Progressive Scanning to allow for customers to scan very large sites, one slice at a time, in order to cover large applications that are problematic to scan in a short window.

### **WAF 2.0 offers:**

**One-click Virtual Patching** – Integrated into Qualys' WAF and WAS solutions, the one-click virtual patching feature addresses both false-positives and the inability to quickly patch vulnerabilities. First, Qualys WAS identifies critical vulnerabilities in web apps, then Qualys WAF allows security teams to virtually patch these vulnerabilities with one-click, and block targeted attacks. This integrated process empowers security teams to quickly protect web apps and minimizes false-positives.

**Out-of-the-box security templates for popular platforms** – Included WordPress, Joomla, Drupal and Outlook Web Application templates are based on the latest Qualys security intelligence, offer fully customizable security policies and make it easy to continuously monitor business-critical web applications.

**Ease of use and flexible deployment** – WAF is available on VMWare, Hyper-V and Amazon Web Services, and includes load-balancing of web servers, health checks for business-critical web applications, custom security rules based on HTTP request attributes, reusable Secure Socket Layer profiles, detailed event log information and centralized WAF management.



Qualys WAS 5.0 and WAF 2.0 are available now as annual subscriptions. Pricing is as follows, based on the number of web applications and virtual appliances:

### **Web Application Scanning**

- Starting at \$1,695 for small businesses
- Starting at \$2,495 for larger enterprises.

### **Web Application Firewall**

- Starting at \$1,995 for small businesses
- Starting at \$9,995 for larger enterprises.

“We use Qualys WAS to scan and secure all our web applications on a continuous basis, and we are pleased with the speed and accuracy of the service,” said David Cook, Chief Security Officer at Jive Software. “We are excited about the Qualys WAF that will allow us to act quickly and respond to threats by using the one-click virtual patching feature to remediate active vulnerabilities.”

# Qualys and Bugcrowd bring automation, crowdsourcing to web app security

Qualys and Bugcrowd announced joint development integrations allowing joint customers the ability to share vulnerability data across automated web application scanning and crowdsourced bug bounty programs.

Many organizations' security strategies have changed to a proactive approach, which includes both automation and human expertise to discover vulnerabilities. To reduce the escalating cost and effort of implementing multiple tools or programs, this joint integration between Bugcrowd Crowdcontrol and Qualys Cloud Platform brings together the scale and efficiency of automated web application scanning (WAS) with the expertise of the penetration-testing crowd in one simple solution.

The Bugcrowd logo consists of the word "bugcrowd" in a white, lowercase, sans-serif font, centered on a solid orange rectangular background.

crowdsourced cybersecurity

Joint customers will be able to eliminate automatically discovered vulnerabilities by Qualys WAS from their list of offered bug bounties and focus Bugcrowd programs on critical vulnerabilities that require manual testing,

effectively reducing the cost of vulnerability discovery and penetration testing.

The initial integration allows Bugcrowd customers who also have Qualys WAS to import vulnerability data from Qualys WAS results directly into the Bugcrowd Crowdcontrol platform and then use that data to optimize their bug bounty program scope and incentives. Further integration with the Qualys Cloud Platform will allow joint customers running a bug bounty platform on Bugcrowd to import unique vulnerabilities from Crowdcontrol into Qualys WAS and have the ability to apply one-click patches using the fully integrated Qualys Web Application Firewall (WAF)

***Joint customers will be able to eliminate automatically discovered vulnerabilities by Qualys WAS from their list of offered bug bounties and focus Bugcrowd programs on critical vulnerabilities that require manual testing.***

"With the move of IT to the cloud and all the digital transformation efforts underway, web apps are exploding and securing these apps is now front and center," said Sumedh Thakar, Chief Product Officer, Qualys. "By combining the automation of Qualys Web Application Scanning (WAS) and Bugcrowd's crowd sourcing platform, organizations can now cover a much larger number of applications and secure them more effectively at a lower cost."

"The pace and complexity of modern application deployment requires organizations to harness both automation and on-demand crowd testing. This integration allows our customers to gain the benefits of both," said Jonathan Cran, Vice President of Product, Bugcrowd. "The integration of Bugcrowd and Qualys data means that this new approach will be easier and lower cost."

The integration of Qualys WAS vulnerability data within Crowdcontrol will be available to joint customers in March, followed by the integration of Bugcrowd data into Qualys WAS and WAF in Q2 2017.



# Qualys Cloud Platform offers two new disruptive services



Qualys announced a major expansion of its Qualys Cloud Platform. New services include File Integrity Monitoring (FIM) and Indicators of Compromise (IOC) detection solutions that enable customers to consolidate even more critical security and compliance functions into a single cloud-based dashboard, and remove the point-solution sprawl that proliferates across their endpoints.

Qualys now combines a comprehensive set of both prevention and detection solutions in the same lightweight Qualys Cloud Agent already deployed for an organization's global asset inventory, vulnerability management, and policy compliance programs.

With Qualys FIM and IOC, customers can instantly add continuous visibility of breaches and system changes to their single-pane view of security and compliance posture already powered by the Cloud Agent.

Qualys File Integrity Monitoring (FIM) – Qualys FIM logs and centrally tracks file change events across global IT systems, delivering users a single-view dashboard from which to detect and identify critical changes, incidents, and audit risks resulting from normal patching and administrative tasks, change control exceptions or violations, or malicious activity.

As a cloud-based solution, Qualys FIM scales visibility and control to a variety of enterprise operating systems without the need to deploy and maintain complex security infrastructure. This allows teams to improve compliance, reduce downtime and limit damage resulting from compromise without the expense of a software-based solution.

## File Integrity Monitoring

**Preconfigured content:** Deciding what to monitor is a challenge for most security teams,

so FIM comes with out-of-the-box profiles based on industry best practices and vendor-recommended guidelines for common compliance and audit requirements, including PCI mandates.

**Real-time change engine:** The Qualys Cloud Agent continuously monitors the files and directories specified in the monitoring profile and captures critical data to identify what changed along with environment details such as which user and process was involved.

**Automated change review:** Qualys FIM provides review workflows and points for external integration to reduce the data users have to look at so they can focus on critical changes and violations first.

## Qualys Indicators of Compromise

Qualys IOC continuously monitors endpoint activity to detect suspicious activity that may indicate the presence of known malware, unknown variants, and threat actor activity on devices both on and off the network. Qualys IOC integrates endpoint detection, behavioral malware analysis, and threat hunting techniques that incorporate a continuous view of an asset's vulnerability posture along with suspicious activity monitoring. It offers:

**Continuous event collection:** Qualys IOC uses the Cloud Agent's non-intrusive data collection and delta processing techniques to transparently capture endpoint activity information from assets on and off the network in a way that is more performant than other solutions' query-based approaches or distributed data collectors.

**Highly scalable detection processing:** Analysis, hunting, and threat indicator processing is performed in the cloud on billions of active and past endpoint events. Those results are then coupled with threat intelligence data from Qualys Malware Labs and third-party threat intelligence sources to identify malware

infections (indicators of compromise) and threat actor actions (indicators of activity).

**Actionable intelligence for security analysts:** Confidence-scored alerts are displayed in the Qualys platform's web-based user interface with contextual asset tags to help security teams prioritize responses for critical business systems.

Qualys FIM and IOC provide significant benefits to security administrators – as delivered by the Qualys Cloud Agent and cloud-based processing platform – over traditional on-premise point security solutions:

**Easy setup and no maintenance:** FIM and IOC modules operate on endpoints via the lightweight Qualys Cloud Agent. Modules can be instantly activated across any or all assets without reinstalling the agent or rebooting the endpoint.

**Minimal performance impact:** The Cloud Agent minimizes performance impact on the endpoint by simply monitoring for file changes and system activity locally, sending all data to the Qualys Cloud Platform for storage, correlation, analysis, and reporting.

**Unified security posture:** Qualys presents FIM and IOC alert data for on-premise assets, cloud server instances, and off-net remote endpoints in a single view that is integrated with the asset's inventory, vulnerability posture, and policy compliance controls, even for assets that are currently offline – thus significantly reducing the time required to effectively detect and respond to threats before breach or compromise can occur.

**Integration with AssetView:** Security analysts can make use of dynamic dashboards, interactive and saved searches, and visual widgets in Qualys AssetView to monitor changes within the context of asset groups.

***Qualys FIM and IOC will both be available in limited beta starting in March.***



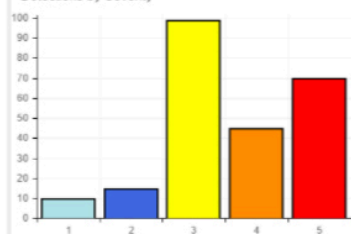
Confirmed Vulns Over Time



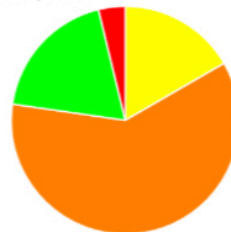
Active Hosts

145

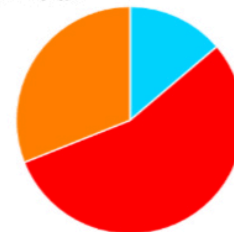
Detections by Severity



Detections by Status



Detections by Type



Hosts Not Scanned in Last 30 Days

Show 10 entries

IP	ID	Last Scanned On
10.10.10.1	2810172	2016-05-14 10:45:00
10.10.10.105	2810176	2016-05-14 10:45:00
10.10.10.11	5527441	2016-05-14 10:45:00

Top 10 Vulnerabilities

QID	No. of Affected Hosts
120878	69
38094	66
None	50
20878	49

## IBM adds Qualys technology to its MSS portfolio

Qualys announced an expanded partnership with IBM that will add Qualys continuous cloud-based IT security and compliance technology to its Managed Security Services (MSS) portfolio.

IBM will integrate Qualys technology to enable its customers with enhanced visibility of IT assets, vulnerabilities and threat data, accelerating how they prioritize remediation and simplify management of their IT security and compliance posture at scale.

Extending digital enterprise infrastructure across global cloud and on-premises deployments requires that security teams gain continuous visibility of assets across diverse IT environments. IBM will add key capabilities of the Qualys Vulnerability Management, Policy Compliance, Continuous Monitoring and ThreatPROTECT to the global threat landscape monitoring operations of its global IBM X-Force Command Centers worldwide.

IBM could also integrate the multitenant Qualys Cloud Platform into its MSS portal and SSO platform, enhancing customers' continuous visibility and prioritization toolsets to more

effectively manage IT security and compliance posture across hybrid public and private clouds.

Qualys app for IBM QRadar offers critical insight into key vulnerability metrics

Qualys launched a new Qualys App for the IBM QRadar Security Intelligence Platform. The new application is freely available to the security community through the IBM Security App Exchange, a marketplace where developers across the industry can share applications based on IBM Security technologies.

Leveraging the Qualys API, customers using the app can automatically import IT asset and vulnerability data from the Qualys Cloud Platform into QRadar for visualization and correlation with security incidents. All of this data can be viewed through customizable visualization widgets that leverage QRadar APIs to graph vulnerability severities and aging, or be searched within the QRadar app for the latest asset and vulnerability data.

# REAL THREAT INTELLIGENCE...

## NOT THREAT INFORMATION

- Operatively-sourced Advanced Threat Intelligence
- Comprehensive, Secure Web-based Platform
- Deep Research – An Extension of Your Security Team
- Proprietary Data Sourcing Delivers Unsurpassed Intelligence

LEARN MORE: **ATI.INFOARMOR.COM**



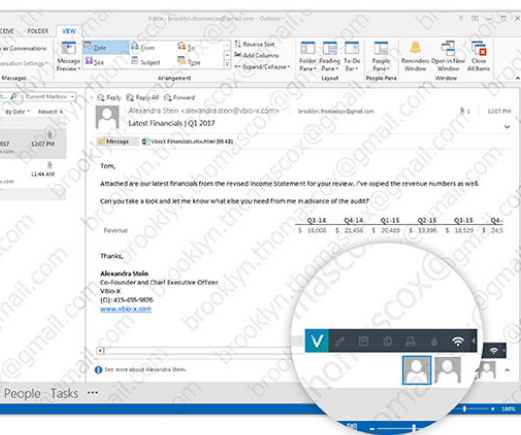




# PRODUCT SPOTLIGHT

## Vera for Mail protects the confidentiality of email messages and attachments

Vera for Mail is an enterprise-grade security solution that lets businesses secure, track, and revoke access to any email they send.



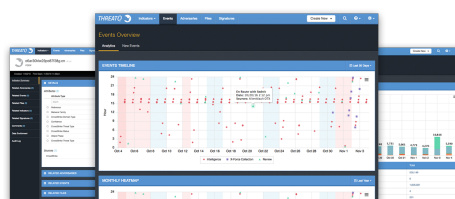
Used by more than 300,000 employees across the Fortune 100, Vera can protect enterprise data, no matter how employees share, communicate, or collaborate.

“In today’s collaborative enterprises, email encryption, audit, and access control is an absolute necessity. Unfortunately, other encryption solutions just aren’t user-friendly or foolproof enough for daily use,” said Ajay Arora, CEO and co-founder of Vera.

## ThreatQ 3.0: A threat intelligence platform with fine-tuned controls

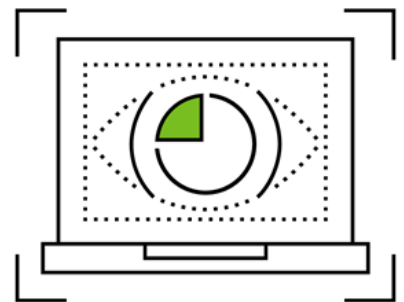
ThreatQuotient announced new ThreatQ platform advancements, a robust Partner Integration Program and Professional Services offerings to answer industry demand to make threat intelligence operational within the context of a company’s specific environment.

“The industry has realized that the aggregation and sharing of threat data is not enough to succeed. Threat intelligence platforms need to do more to support the utility of threat intelligence as part of security operations,” said Leon Ward, Senior Director, Product Management,



ThreatQuotient. “ThreatQ has been purpose-built to support the threat operations within a company. It is designed to help customers focus their resources on the high-risk items that are most pertinent to their business.”

## Self-healing endpoint security as a foundation for visibility



The new Application Persistence product from Absolute provides embedded, self-healing capabilities to third-party endpoint controls such as VPN, anti-virus, encryption, systems management and other critical controls that are too easily compromised.

It leverages Absolute’s patented Persistence technology, embedded in the firmware of more than one billion popular PCs and mobile devices worldwide, giving enterprises and ISVs the power to build more resilient endpoints that self-heal if an application is removed or compromised, and ultimately return to an original state of safety and efficacy without IT intervention.

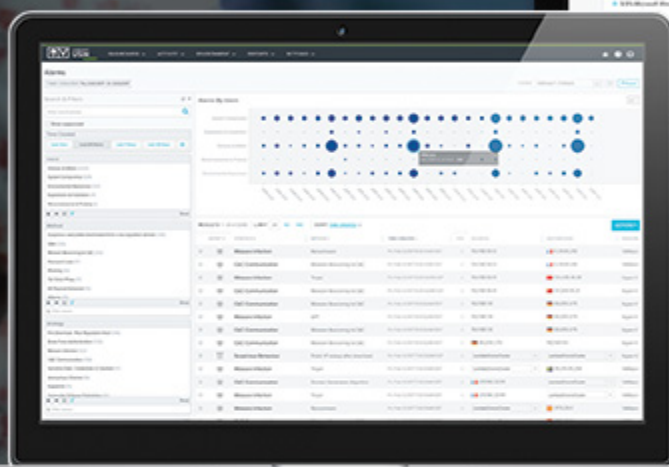


# Discover a Better Way to Detect & Respond to Threats

AlienVault® Unified Security Management™



*Get Complete Security  
Visibility in Minutes*



ASSET DISCOVERY  
& INVENTORY



VULNERABILITY  
ASSESSMENT



INTRUSION  
DETECTION



BEHAVIORAL  
MONITORING



SIEM & LOG  
MANAGEMENT

AlienVault® Unified Security Management™ (USM™) is a comprehensive approach to security monitoring, delivered in a unified platform. The USM platform includes five essential security capabilities that provide resource-constrained organizations with all the security essentials needed for effective threat detection, incident response, and compliance, in a single pane of glass.

Designed to monitor cloud, hybrid cloud and on-premises environments, AlienVault USM significantly reduces complexity and deployment time so that you can go from installation to first insight in minutes!

[www.alienvault.com](http://www.alienvault.com)



## Companies struggle to deploy security for custom applications

As more and more companies migrate their application workloads from their datacenters to IaaS platforms such as Amazon

security departments face a host of new threats and challenges in the move to the cloud. Under cloud's shared responsibility model, IaaS platforms secure the infrastructure but the enterprise is accountable for securing the corporate data, which includes protecting

over 5,000 U.S. consumers at least 16 years old.

The results revealed that consumers are beginning to make purchasing decisions based on the cyber security practices of businesses; and younger generations, who are considered digital natives, see value in companies hiring hackers to help protect consumer data.

## Top phishing targets in 2016? Google, Yahoo, and Apple

For every new phishing URL impersonating a financial institution, there were more than seven impersonating technology companies.

Data collected throughout 2016 by Webroot clearly demonstrates a significant change since 2015, when the ratio was less than one to three. This increase may indicate that it is easier to phish a technology account, and that due to password reuse, they can be more valuable to hackers as a gateway to other accounts. The top three phishing targets in 2016 were Google, Yahoo, and Apple.

Researchers also uncovered a decreasing lifecycle in phishing attacks. The longest-running phishing site was active less than two days, and the shortest was only 15 minutes. Eighty-four percent of all phishing sites were active less than 24 hours.

AWS, Microsoft Azure and Google Cloud Platform, IT pros are worried about the security of the apps, company data, and their jobs.

It doesn't help that while almost 50 percent of custom applications are in the public or hybrid cloud today, companies' IT security professionals are only aware of 38.4 percent of them, according to a recent report by Skyhigh Networks.

Despite growing acceptance of public IaaS platforms, IT

against compromised login credentials, rogue administrators and regulatory violations.

## U.S. consumers' views on cybersecurity

To better understand how Americans think about hacker motivations, consumer versus business security responsibilities, ransomware and the political climates impact on the threat landscape, Kaspersky Lab and HackerOne surveyed







# ARE YOU READY FOR DYNAMIC MULTI-FACTOR AUTHENTICATION?

## ADAPTIVE, CONTEXT-DRIVEN MFA IS HERE.

The days of using cumbersome usernames and passwords as a sole means for authenticating customers are coming to an end. With iovation's authentication solutions, delivering multi-factor security along with an exceptional consumer experience is a reality.

Our service can be easily added to your existing authentication process without adding customer friction, so you can provide your customers with an invisible, hassle-free web experience by recognizing and using their device as an additional factor of authentication.

To learn more, visit [iovation.com/ClearKey](http://iovation.com/ClearKey)



2017 SC MAGAZINE "BEST MULTIFACTOR AUTHENTICATION SOLUTION" FINALIST

[WWW.IOVATION.COM](http://WWW.IOVATION.COM)

# PRODUCT SPOTLIGHT

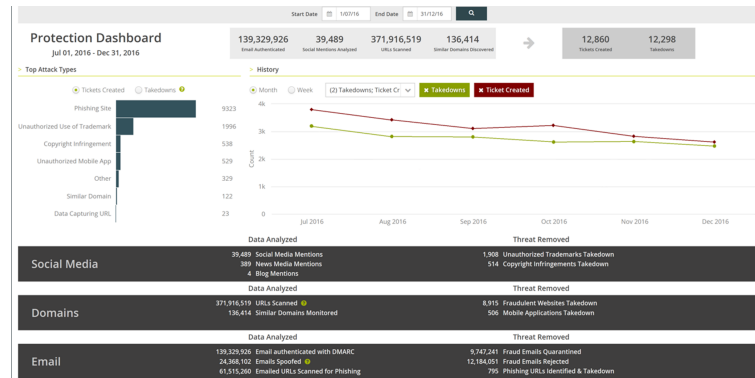
## RansomFree protection software gets key upgrades

Cybereason launched the latest version of RansomFree, the free, anti-ransomware protection software, which works on PCs running Windows 7, 8 and 10, Windows 2010 R2 and Windows 2008 R2.

RansomFree is the ideal anti-ransomware solution for consumers and small businesses such as law and doctor's offices, police and fire departments schools and mom-and-pop shops. It uses behavioral analytics and proprietary deception techniques to target the core behaviors typical in ransomware attacks.

"RansomFree's popularity has us maintaining an aggressive updated schedule. The response to our product has been overwhelmingly positive and we are excited about sharing a free product globally that is helping to stamp out this epidemic," said Uri Sternfeld, lead researcher, Cybereason. "Our goal is to rid the world of ransomware and we will track known and unknown ransomware and will keep delivering game-changing, lightweight, non-intrusive technology to help consumers and small business owners, those most susceptible to cyberattacks."

## Easy Solutions launches digital threat protection suite

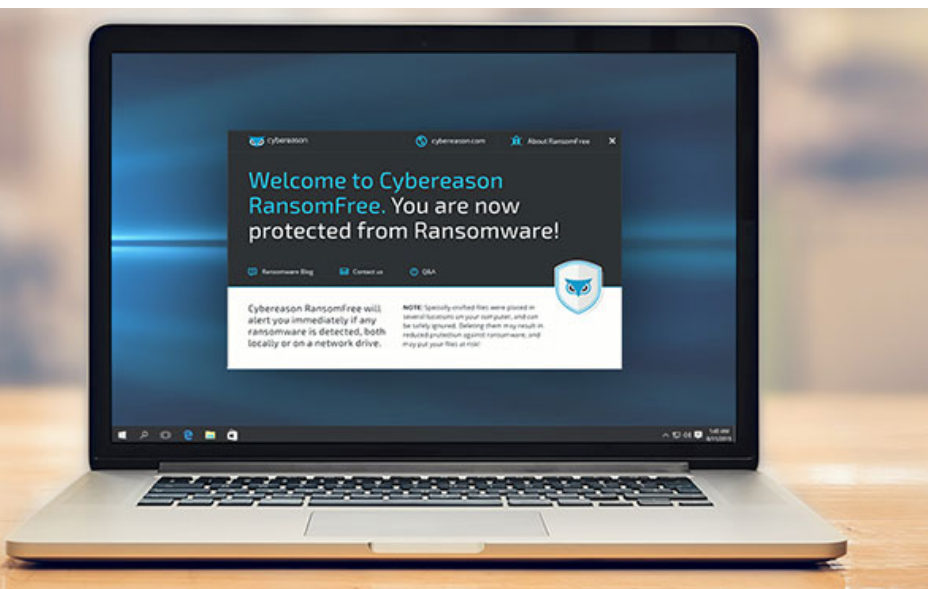


Easy Solutions unveiled its Digital Threat Protection suite. The offering enables organizations with a proactive strategy against fraud by detecting and mitigating attacks aimed at stealing personal information of customers and employees.

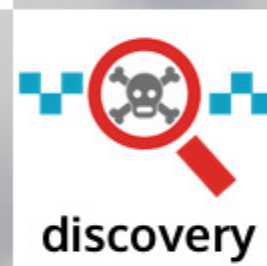
Benefits include continuous, machine-learning driven monitoring and analysis of email, web and social media channels and rapid removal of identified threats.

"Fraudsters are becoming more inventive, and phishing is just the tip of the spear when it comes to attacks that can damage an enterprise's reputation and brand," said

Ricardo Villadiego, CEO, Easy Solutions. "Not only are we providing multi-faceted brand protection, but now we are also delivering it in one easy to access place, so customers can have a holistic view of the threats targeting their organization. At Easy Solutions, we are committed to continue to deliver ever more sophisticated, comprehensive offerings to meet our customers external threat and fraud protection needs."







the only complete **CASB** solution

End-to-end data protection from the cloud to any device.  
Deploys in minutes and works with all major cloud apps.

request a product demo at [bit.ly/bitglassDEMO](https://bit.ly/bitglassDEMO)

---

# Tips on how to address the growing cyber security skills gap

Sophisticated cyber security defenses are increasingly in high demand as a cyber security attack is now viewed as an inevitability. However, a majority of surveyed organizational leaders fear they are ill-equipped to address these threats head-on.

According to a new cyber security workforce study by ISACA's Cybersecurity Nexus (CSX), only 59 percent of surveyed organizations say they receive at least five applications for each cyber security opening. In contrast, studies show most corporate job openings result in 60 to 250 applicants.

Compounding the problem, 37 percent of respondents say fewer than 1 in 4 candidates have the qualifications employers need to keep companies secure.

"Though the field of cyber security is still relatively young, demand continues to skyrocket and will only continue to grow in the coming years," said Christos Dimitriadis, ISACA board chair. "When positions go unfilled, organizations have a higher exposure to potential cyberattacks. It's a race against the clock."

More than 1 in 4 companies report that the time to fill priority cyber security and information security positions can be six months or longer. In Europe, almost one-third of cyber security job openings remain unfilled.

ISACA offers five recommendations to help employers find, assess and retain qualified cyber security talent:

**Invest** in performance-based mechanisms for hiring and retention processes.

**Create a culture** of talent maximization to retain the staff you have. Even when budgets are tight, there are things that can be done that don't impact the bottom line: alternative work arrangements, investment in personnel growth and technical competency, and job rotation to help round out skills and minimize

frustration with repetitive (but necessary) tasks.

**Groom employees** with tangential skills—such as application specialists and network specialists—to move into cyber security positions. They are likely to be highly incented to do so and it can help fill the gap in the long term. Having a path in the organization to do this can be a solid investment, as it can be cheaper to fill those gaps and help support employee morale.

**Engage** with and cultivate students and career changers. An outreach program to a university or an internship program can help with this.

**Automate.** Where security operational tasks can be automated, it can decrease the overall burden on staff and thereby help make best use of staff that an organization already has.







# SECURE ANY CLOUD WITH ARMOR ANYWHERE

**How it works:** cut along the dotted line and apply to your hosting infrastructure responsible for sensitive and regulated data



## Armor Anywhere - Security

Managed Security for any cloud. Anywhere.

Armor Anywhere is a managed, scalable security solution designed for data within public, private, hybrid or on-premise cloud environments. Installed at the OS level and managed by a team of experienced security experts, it prevents data breaches so you can realize your multi-cloud strategy.

**Start Your Secure Cloud Journey Here**

[armor.com](https://armor.com) | (US) 1 877 262 3473 | (UK) 800 500 3167

**ARMOR™**

**THE FIRST TOTALLY SECURE CLOUD COMPANY™**







# YOUR COMPANY SHOULD FOCUS ON THE FUTURE, NOT THE FEAR OF FRAUD



**Protect your customers. Protect your image.**  
Stop cybercriminals from leveraging your brand for their gain.

Online attacks impersonating companies, brands and employees are on the rise. Those attacks threaten customers' sensitive information as well as their trust and loyalty towards an organization. A business with an unsavory reputation suffers financial loss. **Easy Solutions** helps companies develop a proactive strategy to protect against threats. Our unique approach combats fraud attacks from the beginning and deters future attacks.

**EASYSOLUTIONS®**  
TOTAL FRAUD PROTECTION

[www.easysol.net](http://www.easysol.net)



# PRODUCT SPOTLIGHT

## USM Anywhere simplifies security for organizations of all sizes

AlienVault announced the availability of USM Anywhere, an all-in-one SaaS security monitoring platform designed to centralize threat detection, incident response and compliance management of cloud, hybrid cloud, and on-premises environments from a single cloud-based console.



## LaunchKey: Passwordless consumer authentication at scale

ovation announced its LaunchKey mobile multifactor authentication solution. It empowers global consumer brands to improve security and consumer experience by delivering a risk-aware alternative to passwords and two-factor authentication, at scale, via an easy-to-use mobile SaaS solution.



## Insider threat solution for rapid response to in-progress attacks

CyberArk announced advanced insider threat detection capabilities available through the CyberArk Privileged Account Security Solution, to automatically detect and alert on high-risk privileged activity during user sessions and enable rapid response to in-progress attacks.

## Data-centric IoT security for Hadoop Big Data environments

Hewlett Packard Enterprise (HPE) introduced HPE SecureData for Hadoop and IoT, designed to easily secure sensitive information that is generated and transmitted across Internet of Things environments, with HPE Format-preserving Encryption (FPE).


## Advanced machine learning platform preemptively identifies attack pathways

illusive networks announced the illusive Deception Management System (DMS), a machine learning platform that preemptively identifies attack pathways and autonomously creates best-fit deceptions based on continuous real-time environment analysis.

## Inline SSL solution eliminates network blind spots

Gigamon announced an expansion to its GigaSECURE SSL/TLS Decryption solution, with new inline capabilities, bringing enhanced visibility into encrypted data-in-motion. The solution supports both inline and out-of-band decryption. The new set of supported ciphers include Diffie-Hellman (DH), Diffie-Hellman Ephemeral (DHE), Perfect Forward Secrecy (PFS) and Elliptic Curve.



A background image showing a city skyline, likely San Francisco, with a network of white dots and lines overlaid on a semi-transparent globe, symbolizing global connectivity and security.

# DigiCert Security Solutions are Fast, Reliable and Ready to Scale

Whether you need to protect your website, your connected devices or your company's reputation, DigiCert provides a comprehensive suite of scalable, PKI-based security solutions. We understand the complex global nature of your business and innovate to help you issue and manage certificates for reliable identity and encryption across your enterprise network. The world's leading organizations rely on DigiCert to reduce the effort, time and cost needed to secure their valuable business investments.

Learn more at <https://www.digicert.com/mpki/>

