[IN]SECURE

RSA® Conference 2015

SPONSORED BY QUALYS®

FEATURED VENDORS

Below is an index of companies featured in this issue, along with the page number.

Secure Cloud & Mobile in Minutes

BYOD and Cloud Apps are unstoppable trends. The benefits are huge but you lose control of your data.

Regain control with Bitglass.

IT can enable cloud & mobile, securely.

Employees can enjoy privacy and unencumbered mobility.

Secure Cloud

- SaaS Firewall for access control
- Full visibility and alerting
- Track data anywhere on the Internet
- Supports any cloud or internal app

Secure BYOD

- Secure corporate data without MDM or agents
- DLP for sensitive data
- Track data anywhere on the Internet
- Supports Exchange, Office 365, Google Apps etc.

Bitglass deploys in the time it took you to read this.

Sign-up for a free trial at www.bitglass.com

bitglass

This year's RSA Conference proved once again it is the world's most significant information security event. A record number of 33,000 attendees experienced more than 490 sessions, keynotes, peer-to-peer sessions, track sessions, tutorials and seminars, which featured 700 speakers.

On top of that, spread over two expo floors, more than 500 vendors showcased the tools and technologies that will protect personal and professional assets now and in the future.

Featured in this magazine are the most important news and companies from the conference, which will allow you to get an in-depth look at the highlights of the event.

Mirko Zorz
Editor in Chief

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: **Mirko Zorz**, Editor in Chief - mzorz@net-security.org
News: **Zeljka Zorz**, Managing Editor - zzorz@net-security.org
Marketing: **Berislav Kucan**, Director of Operations - bkucan@net-security.org

Photography by RSA Conference and (IN)SECURE Magazine.

THE ULTIMATE THREAT INTELLIGENCE AND TRUSTED COLLABORATION PLATFORM

Your SIEM needs our intelligence. Level the playing field. Use the ThreatStream OPTIC™ platform to aggregate millions of unstructured cyber threats while gaining real-time visibility into your existing security infrastructure, and enable trusted collaboration through a community-vetted threat sharing platform.

Learn more at www.threatstream.com.

THREATSTREAM®

Continuous monitoring of perimeter and internal IT assets

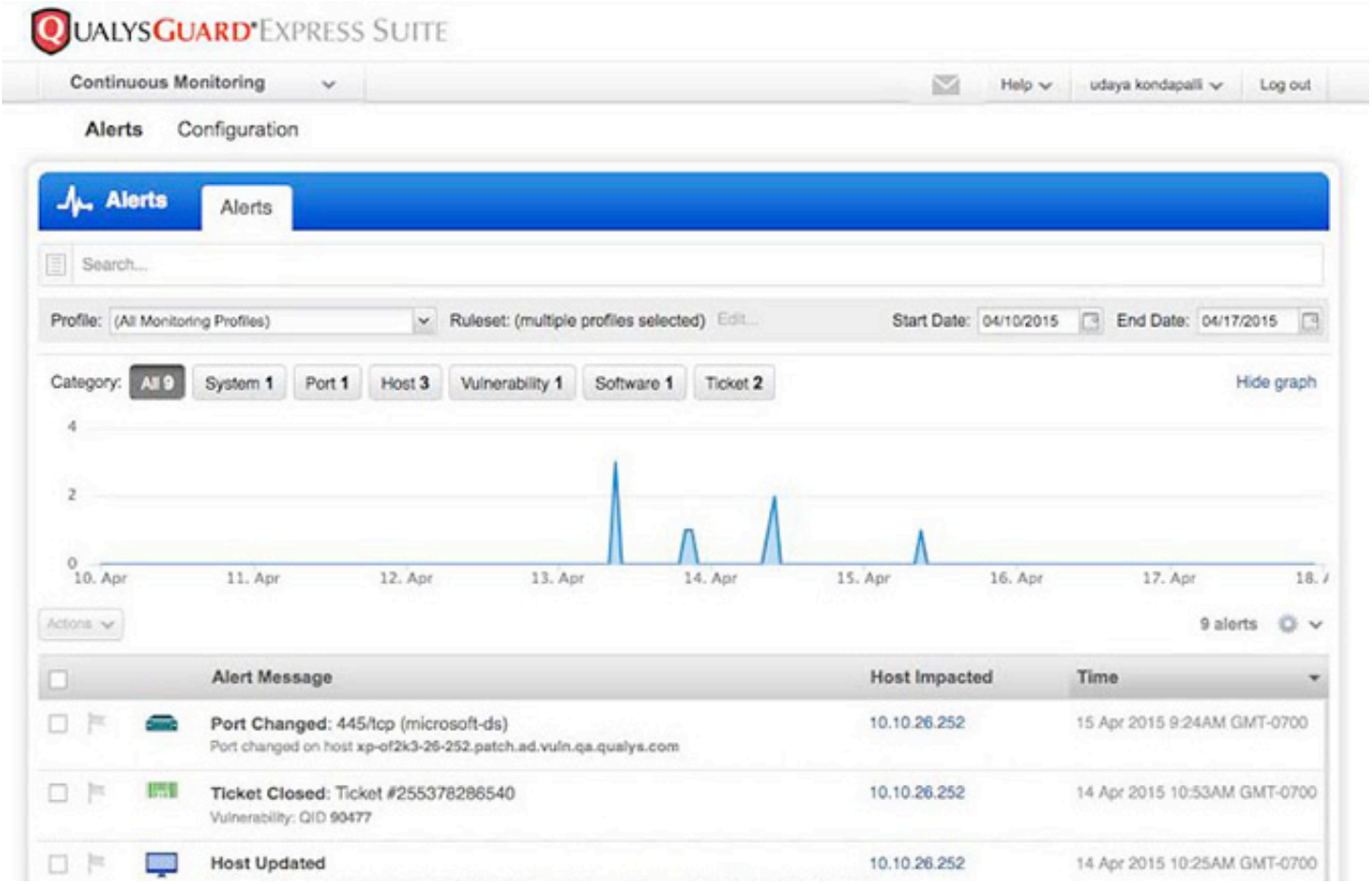
Qualys announced that its popular Qualys Continuous Monitoring (CM) solution for the perimeter now includes internal monitoring capabilities enabling organizations to proactively monitor and get real-time alerts for critical internal IT assets such as desktops, servers and other devices.

Today's cyber attacks are often a result of cyber criminals scanning and attacking networks on a continuous basis, coupled with an event-driven approach to monitoring an organization's perimeter. As a result, vulnerable machines can be exploited within hours with toxic combinations of scenarios that can lead to compromises in their IT environments such as zero-days and phishing scams, which can instantly expose an organization's data. Qualys CM provides a real-time view of an entire organization, and immediately notifies the IT staff as changes are detected so they can take appropriate action.

The solution allows organizations to continuously monitor and respond to changes in their internal environment such as new hosts, OS changes, open ports and services, SSL certificates, as well as changes in vulnerabilities and software.

Qualys CM requires no special hardware and can be set up with a few simple clicks. A user simply needs to identify the host or hosts that need to be monitored, who to alert when states change, and what that change might be. The solution complements the speed of deployment, unparalleled scalability, and accuracy of Qualys Vulnerability Management and other services in the Qualys Cloud Platform.

"Network perimeters are rapidly evolving and expanding. Enterprise data no longer lives solely in the data center but is shared across remote locations and devices, making networks susceptible to cyber attacks," said Philippe Courtot, Chairman and CEO for Qualys. "Our Continuous Monitoring solution helps customers proactively monitor, identify and alert them to unexpected changes in all their critical IT assets before they turn into breaches."




RSAConference2015
SOUTH EXPO


RSA Conference 2015


QUALYS
NETWORK SECURITY
THE NEXT GENERATION CLOUD SECURITY PLATFORM
QUALYS
ASSET DISCOVERY
Know what's on your entire network – at all times


gemalto
SafeNet
POWER UP
RECHARGE HERE
YOUR DATA IS SHOWING. WHAT'S YOUR PLAN?


Identify Your Data with Classification
TITUS
Tackle Your Insider Threat
ANALYZE
PROTECT

Organizations continue to rely on outdated technologies

TechValidate conducted a survey to determine how organizations are implementing NAC policies and security solutions to address today's environments, given the proliferation of cybercrime and growing concerns over insider threats.

The key findings point to outdated approaches to security and a lack of advanced solutions to limit the carte blanche access granted to employees and third parties under older network security models. The survey also indicates that insider threats caused the most actual harm or damage to information security (61%), not outside threats.

BlackVault CYNR: Code and document signing appliance

Engage Black introduced the BlackVault CYNR security appliance. The BlackVault CYNR integrates a Layer 3+ Hardware Security Module (HSM) with application specific code-signing or document-signing functionality to simplify and improve the process of generating, managing and protecting digital signatures.

The appliance is configurable in one of two signing modes: software code or digital documents. As a code-signing appliance, it enables publishers concerned with the potential introduction of spyware, malware, etc. during code distribution to incorporate HSM protection into their code-signing process without the complexity of installing and operating general purpose Operating Systems and HSMs.

For digital signature authentication, the BlackVault CYNR gives legal, financial, real estate and other entities concerned about the cost and ease of forging digital signatures a high level of security within the digital signature process that is both easy to implement and use.

For code-signing applications, the BlackVault CYNR is a "plug-n-play" appliance that allows software developers to easily digitally sign and timestamp their software.

Real-time traffic analysis and inventory of virtualized assets

Catbird Insight, a visualization solution for cloud and on-premise virtual environments that helps organizations rapidly discover, organize and analyze their virtual fabric to reduce security risks, was released.

It provides cloud, network, and application owners, as well as security and compliance teams access to actionable information about their virtual infrastructure. Detailed virtual asset information, network flow information and a unique visualization of both data sets allow for enhanced analytics and improved security posture.

"Companies today want to adopt micro-segmentation to improve their security posture, yet find themselves lacking a good understanding of all the assets within their virtual fabric and missing insight into the baseline connectivity of those assets," said David Keasey, CEO of **Catbird**.

Fox-IT launches cyberthreat management platform

Fox-IT launched its Cyberthreat Management Platform, a suite of solutions, integration tools and expert services designed to provide unified, overarching control of an organization's entire cyberthreat management operations.

The solution was developed directly from the company's 15 years' experience in security research and cyber incident response. It incorporates the same proprietary technology, workflows and intelligence its team of 200-plus security specialists use in cyberthreat management operations for governments, critical infrastructures and global enterprises.

The solution includes capabilities at every level of cybersecurity operations management.

Introducing
TITUS Classification Suite 4

Flexible. Powerful. Secure.

The Industry's Most Advanced Data Classification Solution

TITUS Classification Suite 4 offers an unprecedented level of flexibility and control to make your information protection program a success. From advanced data identification to fine-grained policy control, TITUS provides a security framework to protect your organization's most valuable information assets.

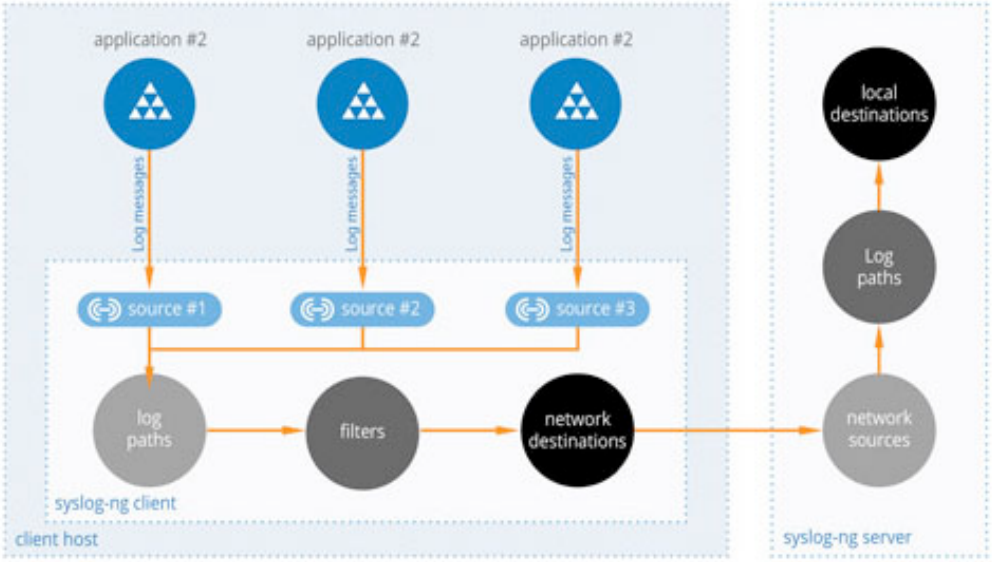
TITUS

For more information visit www.titus.com

BalaBit releases syslog-ng Premium Edition with Big Data support

BalaBit announced an improved version of the company's syslog-ng Premium Edition 5F3 featuring enhanced support for big data environments, which does an exceptional job of managing big data volume, velocity, variety and veracity when delivering log data to large, central data repositories. This release adds support for sending logs directly to Hadoop and allows syslog-ng users the ability to stream logs into the Hadoop Distributed File System (HDFS), eliminating the need to manually load logs into HDFS. Hadoop is powerful tool to store massive amounts data and extract information for a variety of use cases.

"The newest version of syslog-ng can collect data from virtually any source, transform the data, and stream it to Hadoop by connecting to the HDFS cluster; it's not necessary to create any jobs to get the data into HDFS," said Zoltán Györkõ, CEO and co-founder of BalaBit. "You can think of syslog-ng as an Extract Transform Load (ETL) tool for your log data. It's ideal for big data environments because the new version scales really well for large enterprise environments handling a high volume of many types of data. And it can flexibly route data to multiple destinations in hybrid environments. We're very pleased with the scalability this product offers customers."



Raytheon delivers end-to-end visibility to address cyber threats

Raytheon announced a new suite of solutions that can change the way companies address cybersecurity by helping enterprises operate in the face of sophisticated cyber threats.

The SureView product suite combines human and machine learning to prevent insider threats, reduce the amount of time an external threat remains in an organization's network, and provide actionable intelligence that helps eliminate future attacks.

Dave Wajsgras, President of Raytheon Intelligence, Information and Services said: "Today's launch reflects our firm belief the time has come for commercial customers to have the same caliber of protection that helps our traditional customers remain resilient in the cyber domain."

"The SureView portfolio evolved through a combination of capabilities Raytheon acquired and unique technologies developed in-house to protect its traditional customer set and the company's own systems and data," stated Ed Hammersla, president of Raytheon Cyber Products. "By delivering proven technologies that scale to meet the most demanding requirements, Raytheon's SureView products bridge the gap between defense-grade and enterprise cybersecurity."


Your Data is Showing...
What's your Plan?
HEALTH RECORDS
CORPORATE STRATEGY
DOCUMENTS
TECHNICAL PLANS
CREDIT REPORT
BANK ACCOUNT NUMBER
SOCIAL SECURITY NUMBER
HEALTH RECORDS
USER NAME
LEGAL DOCUMENTS
SOCIAL SECURITY NUMBER
HEALTH RECORDS
DATE OF BIRTH
PASSWORD
BANK ACCOUNT NUMBER
HEALTH RECORDS
SOCIAL SECURITY NUMBER
HOME ADDRESS
CORPORATE STRATEGY
DATE OF BIRTH
LEGAL DOCUMENTS
CREDIT CARD NUMBER
HOME ADDRESS
HEALTH RECORDS
FULL NAME
CREDIT CARD NUMBER
Enterprise organizations are in possession of more sensitive information than ever before and data breaches are inevitable. The new priority of CISOs around the globe is how to "secure the breach" so organizations can ensure that any data obtained from a breach is encrypted and therefore useless.
Learn how to
Secure the Breach in 3 steps!
www.securethebreach.com
SafeNet.
gemalto
security to be free


Entrust Datacard
Trusted Identities | Secure Transactions
MANAGED PKI &
INTERNET OF THINGS


LOG
SYSLOG-NG
ARE YOU SEEING THE COMPLETE PICTURE WITH YOUR LOG DATA?
PAM
SHELL CONTROLL BOX
DO YOU WANT TO BETTER MONITOR YOUR PRIVILEGED USERS?


The
CRYPTOGRAPHERS' Panel

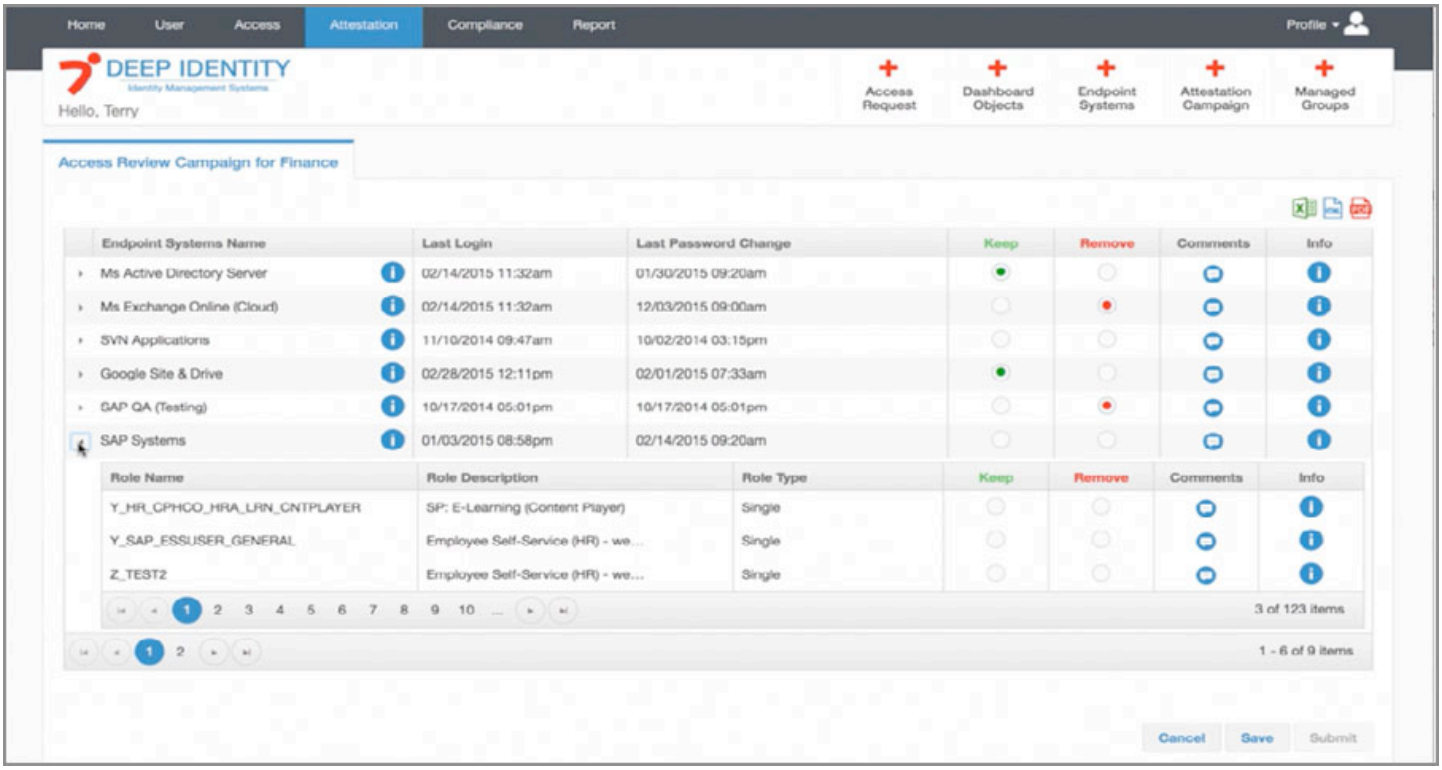
Identity, data governance across all apps, systems, and devices

Deep Identity announced their expansion into London, UK, and the release of version 5 of their Identity and Data Governance Suite.

Key features of the new software suite include an improved User Interface, a Self-service Portal for iOS and Android, and certified support for leading SQL platforms and integration with Deployment Manager of the Deep Identity Community Cloud.

Additionally slated for release is BYOD (Mobility) support. This will allow enterprise users to perform password resets, unlock accounts, perform profile administration and access request approval via the Identity Portal.

Deep Identity is deploying tools and wizards to speed up implementations. Phase-1 will include extended schemas, creation of custom access request forms, creation of custom workflow processes and creating custom connectors. The Deployment Manager will also feature the Lifecycle Manager to version all items being deployed across various environments. This will be integrated in tandem with code migration and configuration backup to the Deep Identity community cloud.



Making password databases impossible to steal

A new technology, called Blind Hashing, that prevents offline password attacks by making databases impossible to steal, has been introduced by **TapLink**.

TapLink is completely invisible to the end-user, easy to integrate, has minimal impact on back-end systems, and works in conjunction with existing password defenses, systems and processes.

The Blind Hashing technology transforms a password hash into a lookup function within a massive pool of completely random data. The result of the lookup is used to decrypt the hash and allow the authentication process to be completed with no latency impact to the log in process.

A petabyte-sized data pool acts as a "data anchor" to prevent an attacker from ever cracking a single password. In order to begin the password cracking process, an attacker would have to steal the entire data pool, spanning hundreds of SSDs across multiple data centers. In what pundits have dubbed "security by obesity", the TapLink data pool is so large that simply trying to transfer it over the network at full line rate would take years.

SOLUTIONARY®

AN NTT GROUP SECURITY COMPANY

Services and Intelligence to Optimize Security and Mitigate Risk.

- Managed Security Services
- Targeted Threat Intelligence
- Security Log Monitoring
- Log Management
- Critical Incident Response
- Professional Services

Visit Solutionary.com for More Information

RSA Conference named Waratek most innovative new company.

Marking the 10-year anniversary of Innovation Sandbox Contest since the event launched at RSA Conference 2005 as Innovation Station, Waratek was selected from a group of 10 finalists.

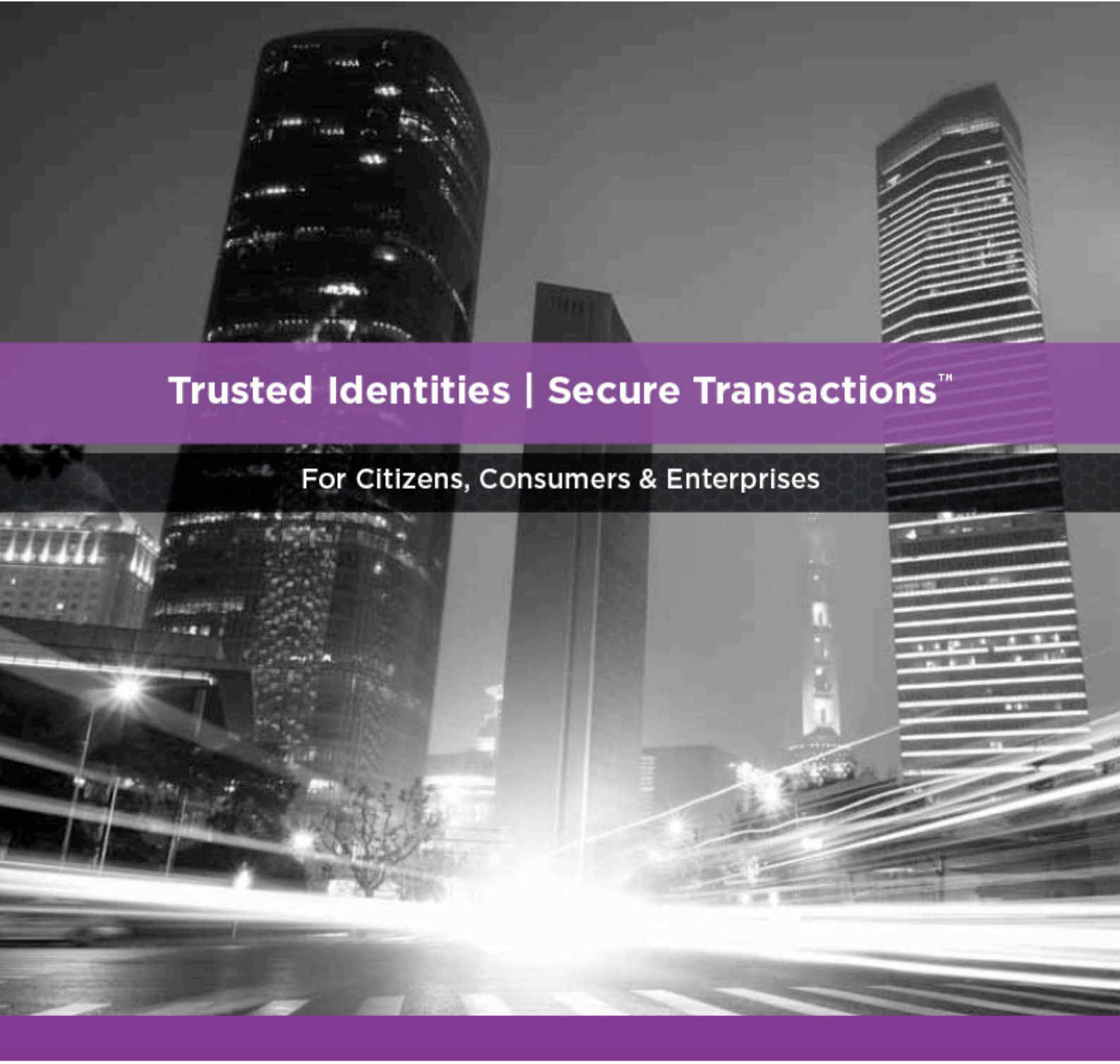
In a first for the event, acknowledging the competitiveness of this year's field, Ticto was also named as the runner up. The annual conference competition is a half-day program during which up-and-coming startups grab the spotlight and demonstrate groundbreaking security technologies to the broader RSA Conference community. Past winners include Sourcefire, Imperva, and, most recently, RedOwl Analytics.

Waratek won the award based on its ability to clearly demonstrate strengths in addressing the market's need for better application protection against sophisticated attacks without having to install network devices, make code changes or greatly impact performance.

"This is a huge honor and award for the Waratek team," said Anand Chavan, co-CTO of Waratek. "We were not anticipating this level of competition and every company that presented here is doing great things. It feels great to have this panel of judges validate our approach to this challenging security issue."

"RSA Conference has always been dedicated to encouraging the discussion of new ideas and providing support for groundbreaking information security technologies that push the industry forward. It proved that once again, as Innovation Sandbox Contest's 10 finalists showcased some of the most innovative security solutions," said Sandra Toms, vice president and curator of RSA Conference.

"Coming out on top, Waratek demonstrated that they were the most innovative new company by highlighting the need for their unique approach to application security."



Trusted Identities | Secure Transactions™

For Citizens, Consumers & Enterprises

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. They also expect the ecosystems that allow this freedom and flexibility to be entirely reliable and secure. Entrust Datacard offers the trusted identity and secure transaction technologies that make these ecosystems possible.

To learn more, visit entrustdatacard.com

Entrust Datacard™

New cloud security certification from (ISC)2 and CSA

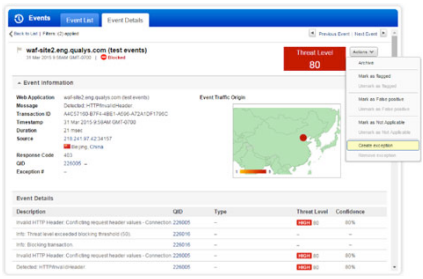
(ISC)2 and the **CSA** announced the new Certified Cloud Security Professional (CCSP) certification. The CCSP represents the advanced skills required to secure the cloud, while establishing an international standard for professional-level knowledge in the design, implementation and management of cloud environments.

CSA's CCSK provides an indicator of baseline cloud security knowledge appropriate for almost any IT position. The CCSP credential builds upon many of the areas covered by CCSK in order to provide deeper knowledge derived from hands-on information security and cloud computing experience. It validates practical know-how skills applicable to those professionals whose day-to-day responsibilities involve cloud security architecture, design, operations and service orchestration.

The CCSP credential is intended for professionals who are heavily involved in cloud security via roles that are accountable for protecting enterprise architectures.

To attain CCSP, applicants must have a minimum of five years of experience in IT, of which three must be in information security and one year in cloud computing.

Qualys takes step towards complete automation of web app security



Qualys announced Qualys Web Application Firewall (WAF) version 2.0 that comes fully integrated with the Qualys Web Application Scanning solution (WAS).

The new release includes virtual patching capabilities to enable organizations to fine-tune security policies, remove false positives and customize rules leveraging vulnerability data from the Qualys WAS.

Qualys WAF also includes customizable event response, helping customers evaluate and create exceptions to web events to better prioritize and mitigate vulnerabilities, making it one of the first end-to-end web application security services to combine WAF security rules and policies with WAS data to address web application security threats.

As hackers continue to find new ways to penetrate web applications, WAFs can detect, alert and block known attacks. With the latest version of Qualys WAF, users can now create "virtual patch" rules in direct response to their Qualys WAS findings, to enable rapid false positive resolution, as well as customization of security rules tailored for the organization's environment. This helps customers tune security policies, remove false positives, and easily customize WAF security rules for web applications.

The portable secure desktop: tVolution Mini

Becrypt launched tVolution Mini. The device is smaller than a mobile phone, but has the power of a PC, and transforms a monitor or TV into a smart device for securely accessing corporate applications and data.

Although it looks like a USB stick or credit card, tVolution Mini is a PC in its own right, which means it doesn't rely on another device's operating making it more secure. It enables organizations to provide staff or partners with a low cost computer to access a corporate network securely, protecting the systems from the risk of malware inherent with users accessing corporate resources from home or unmanaged PCs.

Requiring less than 5 Watts of power, tVolution Mini is an exceptionally low power consuming device that can help your organization to reduce power usage, while still retaining full functionality for users.


EndpointProtector.com
Data Loss Prevention (DLP)
Device Control
Mobile Device Management (MDM)
ENDPOINT PROTECTOR
EndpointProtector.com


RSA Conference 2015


bitglass
Total Data Protection
Outside the Firewall
elastica


DEEP IDENTITY
Why Deep Identity?


NTT Group
Global Reach. Local Delivery.


AhnLab
CHANGE


RSAConference2015

ARE YOU ADEQUATELY PROTECTED AGAINST DDoS ATTACKS?

DOSarrest's fully managed, cloud-based DDoS protection service guarantees website availability and keeps attackers out!

Traffic scrubbing centers in
London, NYC,
LA and Singapore.

DOSarrest has been
protecting websites against
DDoS attacks since 2007

DDoS attacks are larger and more sophisticated than ever before. It can paralyze your website, leaving you unable to process transactions, accept payments, and disseminate information. A combination of attack methods can lead to data loss, ID theft, and fraud.

DOS arrest
Internet security
www.DOSarrest.com

US/CAN Toll Free: **1.888.818.1344** * Press 1 for Sales
UK Free Phone: **0800 086 8812** * Press 1 for Sales
Singapore Toll Free: **800 - 101 - 1796** * Press 1 for Sales
Email: **sales@DOSarrest.com**

Head office:
Vancouver, B.C., Canada

Use of encryption continues to rise

The use of encryption continues to grow in response to consumer concerns, privacy compliance regulations and on-going cyber-attacks and yet there are still major challenges in managing key across what are the mostly fragmented and tactical deployments of encryption technologies, say the result of **Thales**' 2015 Global Encryption and Key Management Trends Study.

“Encryption usage continues to be a clear indicator of a strong security posture but there appears to be emerging evidence that concerns over key management are becoming a barrier to its more widespread adoption," commented Dr Larry Ponemon, chairman of The Ponemon Institute. "In this study we drilled down into the issue of key management and found it continues to be a huge operational challenge. What is clear is that many organizations lack formal ownership and accountability when it comes to key management which is very concerning when you consider the value of the data being protected and operational implications of losing or mismanaging keys.”

Automated protection of enterprise email, docs and data

TITUS launched TITUS Classification Suite 4, a significant new release of its flagship data identification and information protection suite. Already in use by the French Ministry of Defense and others, the new solution uses content and context to automatically classify and protect information as it is handled by users, and allows manual and guided classification for flexibility and user engagement. Fine-grained policy control and comprehensive metadata capture also leverages overall security investment, improves data management and increases regulatory compliance.

The suite offers a new flexible policy engine that can apply complex rules to protect information without getting in the way of business process or requiring users to remember security policies. Administrators can set up policies to, for example:

- classify email based on recipients
- protect email based on the content or classification of attachments
- classify and protect documents based on content, filename or location
- prevent printing of sensitive documents on non-secure printers.

Customizable, easy-to-use alerts warn users of special information handling conditions or possible impending security violations.

The suite also integrates with DLP solutions, allowing enterprises to optimize security policy, focus on high-risk areas, and capture retention-related metadata for informed archiving or deletion. New integration capabilities, such as with the Intel Security Data Exchange Layer (DXL), will allow organizations to enhance their behavioral analytics and reporting capabilities, which can help them uncover malicious insider threats.

Gemalto's solutions challenge today’s security thinking

Increasingly more applications, data and services are being built, managed and stored both inside and outside of the enterprise and accessed by individuals anytime, anywhere, and from any device. The disappearance of a defined perimeter has created complexity for security professionals that has been compounded even further by threats becoming more sophisticated.

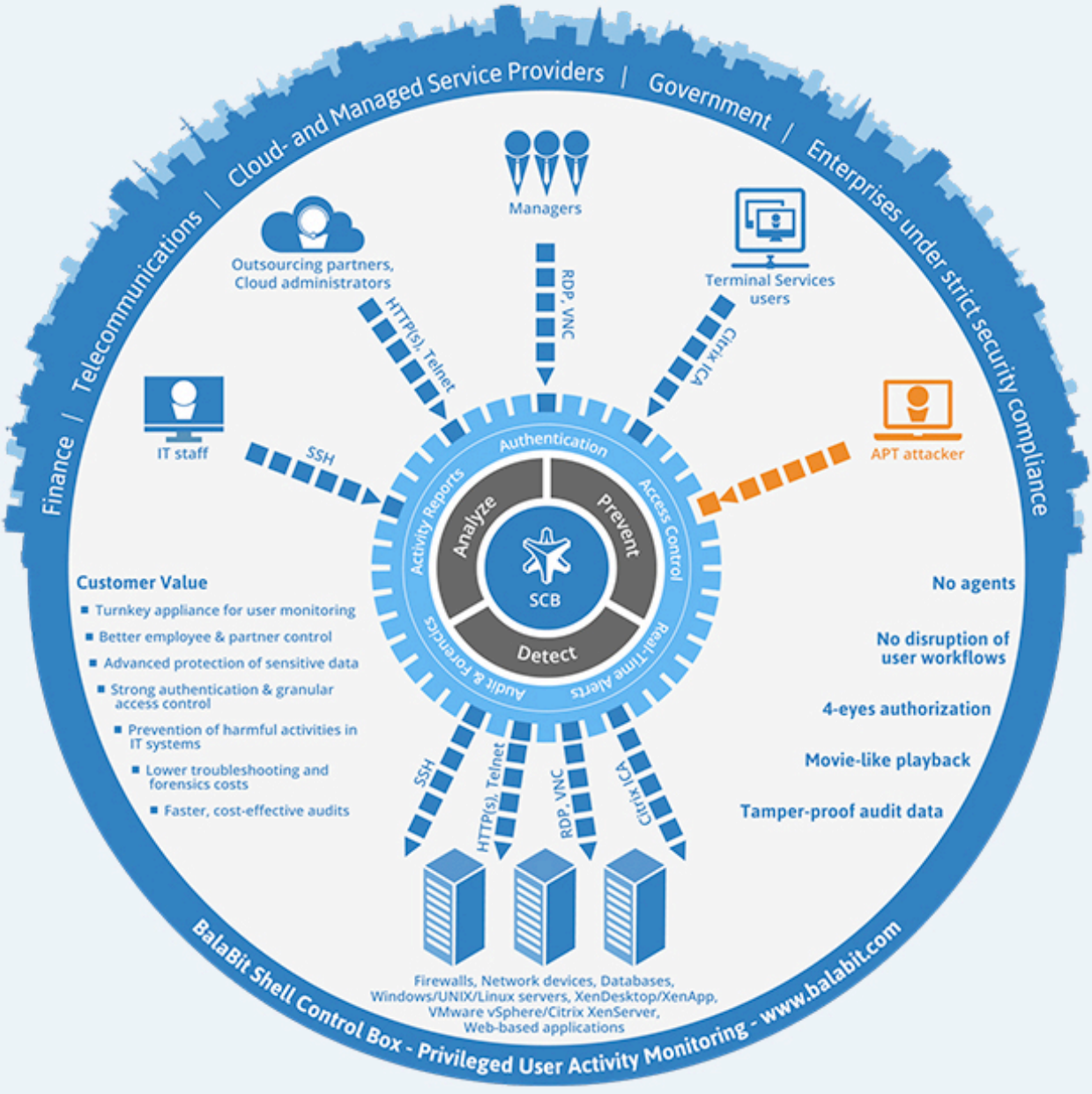
Gemalto's SafeNet Identity and Data Protection solutions help customers tackle the perimeterless enterprise and "Secure the Breach" with a data-centric approach to the protection and control of their sensitive information, from the core of the network to its furthest edge.

From the physical and virtual data center, Gemalto's SafeNet data encryption solutions help organizations remain protected, compliant, and in control with offerings that secure sensitive information in applications (ProtectApp), cloud environments (ProtectV), databases (ProtectDB), network drives and file servers (ProtectFile), storage systems (StorageSecure), and in motion (High-Speed Network Encryption).

BalaBit
IT Security
GUARDING YOUR BUSINESS

Presented at #RSAC:

TOP 10 Best Practices regarding Privileged Activity Monitoring by BalaBit



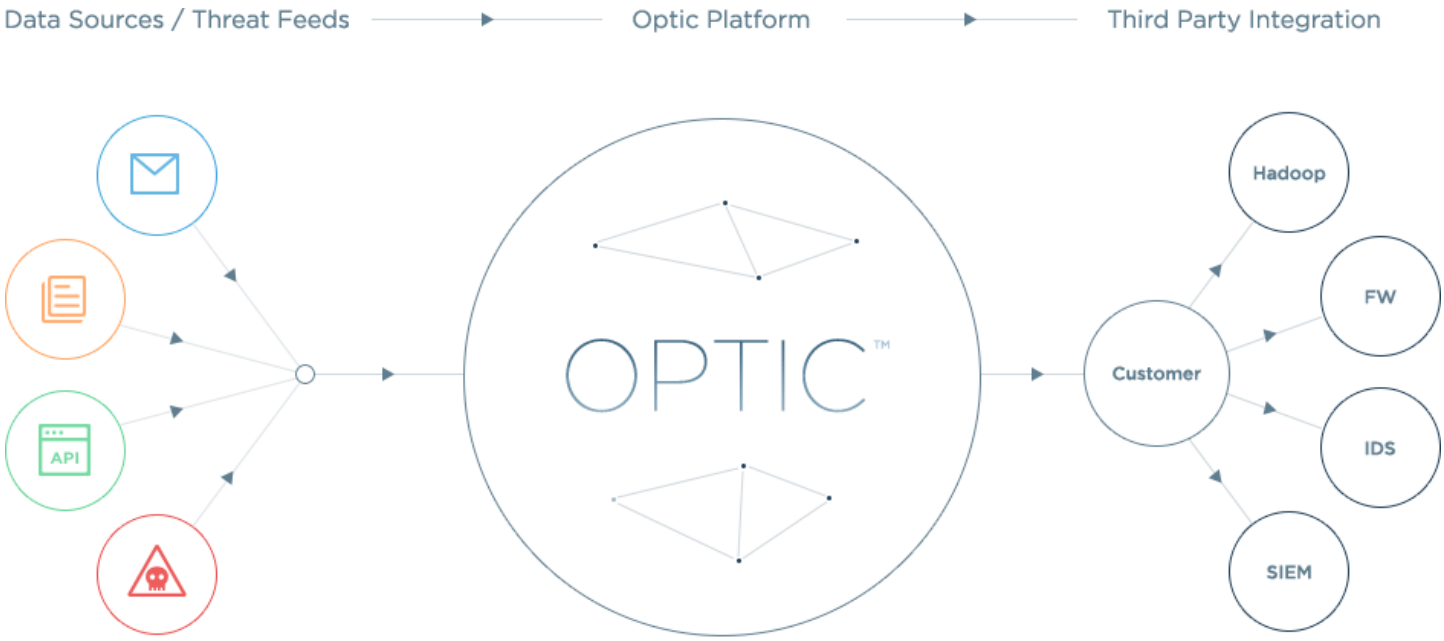
Download the "The Essential Guide to Privileged Activity Monitoring" study for free at https://balabit.com/rsa.

Apple Watch app for managing threat intelligence on-the-go

ThreatStream announced the first iOS threat intelligence app for the Apple Watch. The app, which is also available for the iPhone and iPad, provides full access to the ThreatStream Optic threat intelligence platform dashboard and displays, and enables users to take action with a simple tap of the screen or voice command.

The iOS app will enable SOC analysts to receive and respond to threat alerts triggered by the Optic platform regardless of where they are. Users of the app can receive notifications and alerts in real-time, untethering from the displays of their security controls without jeopardizing their ability to see and respond to threats immediately.

ThreatStream Optic is the first threat intelligence platform that manages the entire life-cycle of threat intelligence, from multi-source acquisition to operational integration across the entire eco-system of existing security devices. Optic enables enterprises and government organizations to seamlessly aggregate and analyze threat intelligence and automatically integrate the information into their security infrastructure and controls.



Early-warning-as-a-service for extended enterprise networks

Norse introduced the Norse Intelligence Service, a fusion of automated and human threat monitoring and analysis that offers “early warning as-a-service” for the very large extended enterprise networks.

The Norse Intelligence Service helps Fortune 500 companies and government organizations address this by combining a globally distributed network of attack sensors — the Norse Intelligence Network — with automated actuarial-based risk scoring and scalable, on-demand human intelligence analyst expertise.

Cyphort combines APT detection with lateral movement

Cyphort announced the availability of Cyphort Advanced Threat Defense Platform 3.3, which includes malware lateral movement detection, the ability to combine advanced targeted attacks and APT detection with lateral movement.

Cyphort combines the inspection of internal enterprise traffic with the innovative behavioral analysis array of sandboxes and machine learning analytics currently protecting enterprises from internet-based threats. This approach results in a clear picture of the impact and spread of advanced attacks while minimizing the false positives and false negatives.


How Do We


RSA
Conferenc
2015


DOS arrest
internet security
PREVENT A
DDoS ATTACK
FROM TAKING DOWN
YOUR WEBSITE


2800
WATCH
THREATSTREAM


RSAConference2015
SOUTH EXPO

Simplified VPN, web access for authorized users via push notification

Entrust Datacard introduced a new push authentication capability in its Entrust IdentityGuard Mobile platform that allows authorized users to more easily and securely access VPNs and websites with their mobile phones or tablets.

Instead of introducing another easily misplaced or forgotten hardware token, introducing complex passwords or series of security questions, the new IdentityGuard Mobile push authentication sets up a secure session using a mobile device by instantly pushing alerts to the users to verify login right as they access their VPN network. With a simple "OK" acknowledgement from the user, the VPN or website access is securely established – making it much faster and more convenient to authenticate users and secure the connection.

"Due to the changing threat landscape, addressing regulatory compliance and breach threats means companies need to continuously secure employee access to company networks and applications – especially as the workplace becomes more mobile and ubiquitous," said David Rockvam, vice president of product management for Entrust Datacard. "It only makes sense that authentication solutions align with that new reality. At Entrust Datacard, we are transforming mobile devices into secure, simple to use, always in hand authenticators to ensure data is protected for businesses and people."

How attackers exploit end-users' psychology

Proofpoint released the results of its annual study that details the ways attackers exploit end-users' psychology to circumvent IT security. Key findings include:

Every organization clicks. On average, users click one of every 25 malicious messages delivered. No organization observed was able to eliminate clicking on malicious links.

Middle management is a bigger target. Representing a marked change from 2013 when managers were less frequently targeted by malicious emails, in 2014 managers effectively doubled their click rates compared to the previous year. Additionally, managers and staff clicked on links in malicious messages two times more frequently than executives.

Sales, Finance and Procurement are the worst offenders. Sales, Finance and Procurement (Supply Chain) were the worst offenders when it came to clicking links in malicious messages, clicking on links in malicious messages 50-80 percent more frequently than the average departmental click rate.

Clicks happen fast. Organizations no longer have weeks or even days to find and stop malicious emails because attackers are luring two-out-of-three end users into clicking on the first day, and by the end of the first week, 96 percent of all clicks have occurred. In 2013, only 39 percent of emails were clicked in the first 24 hours; however, in 2014 that number increased to 66 percent.

NetIQ makes it easy to grant and revoke access to sensitive data.

In today's ever-changing business world, employees and contractors frequently come and go. And because there's no simple way to turn complex systems on and off, it's easy for users (and former employees) to retain access to data they no longer need. If only there was an easy way to control who can access what, when. There is, with NetIQ Identity-Powered Solutions. Granting access based on policy, NetIQ® Identity Manager can easily, even automatically, revoke access rights once they're no longer needed—making sure your sensitive data stays protected.

Put the Power of Identity™ to work.
www.netiq.com/automatedaccess

NetIQ.

Lack of skilled infosec pros creates high-risk environments

82 percent of organizations expect to be attacked in 2015, but they are relying on a talent pool they view as largely unqualified and unable to handle complex threats or understand their business. 35 percent are unable to fill open positions.

Based on a global survey of 649 cybersecurity and IT managers or practitioners, the **ISACA** and **RSA Conference** study shows that 77 percent of those polled experienced an increase in attacks in 2014 and 82 percent view it as likely or very likely that their enterprise will be attacked in 2015. At the same time, these organizations are coping with a very shallow talent pool. Only 16 percent feel at least half of their applicants are qualified, and 53 percent say it can take as long as six months to find a qualified candidate.

Evasive malware goes mainstream

Lastline Labs conducted analysis of hundreds of thousands of malware samples collected in 2014.

Dr. Christopher Kruegel, Chief Scientist at Lastline told (IN)SECURE: "Our Lastline Labs report shows that evasive malware, custom-engineered to elude traditional sandboxes, has gone from niche to mainstream. At the same time, signature-based AV scanners became considerably worse at detecting the 1% least-detected malware over the past year. This indicates that both first generation sandbox solutions and signature-based AV systems aren't able to adapt to new advanced and evasive threats."

Individual malware samples are including more evasive behaviors, often using a combination of 500+ evasive behaviors. While a year ago only a small fraction of malware showed any signs of evasion, today a sizeable portion is evasive. And while evasive malware a year ago tended to leverage at most two or three evasive tricks, much of today's evasive malware is tailored to bypass detection using as many as 10 or more different techniques.

Protecting identities from the endpoint to the cloud

RSA launched the RSA Via family of Smart Identity solutions, engineered to combine authentication, identity and access management, and identity governance silos into one unified solution that allows dynamic, end-to-end identity management across diverse systems and users. The newest offering under the RSA Via family is RSA Via Access, a SaaS-based solution that is designed to allow users to more easily and securely authenticate themselves by taking advantage of multiple convenient authentication methods resident within their into mobile devices.

Network discovery and visibility for massive enterprise networks

Auconet unveiled its new Enterprise Security Foundation (ESF) that fortifies security for both partners and enterprises.

ESF provides third-party applications with Auconet's network asset discovery and visibility engine that underpins security solutions with granular, real-time data on every device, link, endpoint, and port.

The addition of this data on the network infrastructure substantially enriches security tools with its single-source-of-truth about all network assets, enabling deeper and broader enterprise security.

SecureDoc Cloud removes security concerns related to cloud file sharing

WinMagic introduced security software that encrypts and manages how files are shared via cloud file sharing services such as Dropbox or Box.

SecureDoc Cloud leverages WinMagic's endpoint-focused key management capability; by giving full rights of encryption keys to the enterprise, the need for file-sharing passwords when combined with pre-boot authentication is eliminated and a user's encryption experience is completely transparent.

ENDPOINT PROTECTOR

Data Loss Prevention at its best

Get your complete security in a simple appliance with powerful and rock solid foundation for your sensitive data.

Device Control

Protect the entire network

USB monitor and lockdown for Windows, Mac and Linux.

Content Aware Protection

Precise control over transfer of documents on Windows and Mac OS X computers

Enforce corporate policy by ensuring documents containing confidential data are not shared via online applications outside the company.

Enforced Encryption

Additional security for data copied on USB devices from Windows and Mac OS X computers

Make sure that users copy sensitive data only to encrypted USB devices to avoid data leakages in case devices get lost or stolen.

Mobile Device Management

Control iOS and Android devices to secure corporate data

Secure your mobile devices and keep a close eye on sensitive enterprise data both inside and outside companies' walls.

COSOSYS

www.**endpointprotector**.com

Phone: +40-264-593 110
E-mail: feedback@cososys.com
CoSoSys Ltd. • Haiducului St.6 400040 Cluj-Napoca, Romania


NetIQ


NETWORK SECURITY
QUALYS
WEB APP SECURITY


PACSAT


Innovation
Sandbox

Cloud agent platform for continuous IT asset inventory, security and compliance

Qualys announced the launch of Qualys Cloud Agent Platform (CAP), which extends Qualys' Cloud Security and Compliance Platform with lightweight agents to continuously assess security and compliance of organizations' global IT infrastructure and applications.

The Qualys Cloud Agent combines the power of its Cloud Platform with lightweight agents that are extensible, centrally managed and self-updating, and provides organizations with a flexible solution to assess and address the security and compliance of their IT assets in real time, whether on-premise, cloud-based or mobile endpoints.

IBM brings cyber threat analytics to the cloud

IBM is bringing its Security Intelligence technology, IBM QRadar, to the cloud, giving companies the ability to prioritize real threats and free up critical resources to fight cyberattacks. The new services are available to clients through a cloud-based SaaS model with optional IBM Security Managed Services to provide deeper expertise and flexibility.

The new offerings are backed and delivered through IBM's platform of managed security services, handling over 15 billion security events per day for over 4,000 clients around the world. IBM Security experts, located in ten global SOCs, are available on demand 24x7.

Barracuda makes its NG Firewall manageable via iOS app

Barracuda has released the latest version in its NG Firewall product line, which includes new features and updates designed to simplify setup, administration and management. The Barracuda NG Firewall now includes self-service configuration for remote end users using OS X, Windows and iOS to configure their VPN connection in a few clicks. The latest version also allows administrators to activate SafeSearch and YouTube for Schools enforcement in the firewall rules settings. With the new version, Barracuda released the new Barracuda NG Firewall Remote iOS application, designed for system administrators needing simple access to NG control centers from iOS devices.

Automate root cause prevention of network compromise

FireMon announced significant advancement of its core platform through the introduction of Security Manager 8.0, which leverages highly automated analysis and monitoring of security infrastructure to identify and resolve emerging gaps in network defense. With the ability to blend machine learning, correlation, and natural language in a simple, workflow-centric interface to unearth strategic network security operations and management trends, the addition of Immediate Insight's capabilities to Security Manager 8.0 and its integrated modules further empowers organizations to mitigate critical network risks.

High-profile data breaches made most CEOs re-examine security programs

There has been increased board- and C-level interest in information security programs in light of recent high-profile data breaches such as those affecting Sony, Anthem and JP Morgan, the results of a new survey have revealed. As the severity and consequences of data breaches intensify, **Netskope** surveyed a hundred infosec professionals attending RSA Conference 2015 and found the majority of respondents' board of directors and CEOs have taken active interest in understanding and improving their company's security programs.

"As more information is disclosed and media follow every detail of mega breaches, there's an incredible amount to learn," said Sanjay Beri, CEO, Netskope. "I'm encouraged knowing that recent high-profile data breaches have incited conversations between board-level decision-makers and security teams, and action is being taken to prevent similar breaches."

DEEP IDENTITY

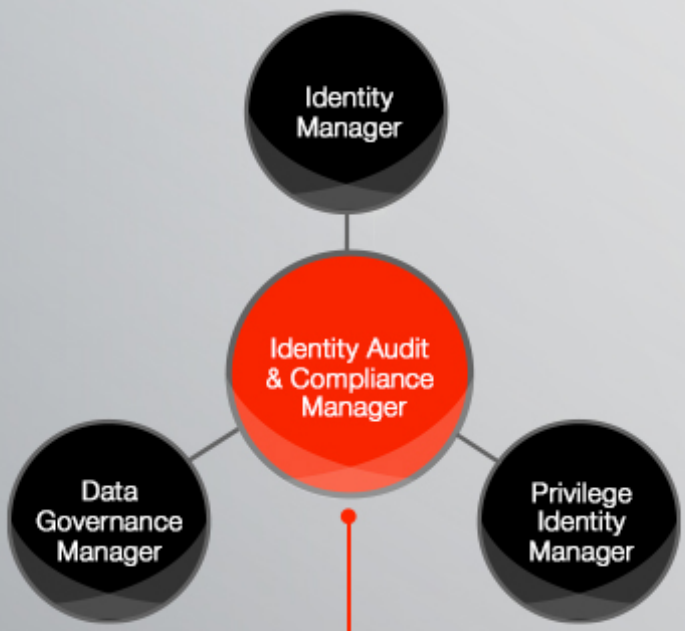
IDENTITY GOVERNANCE | DATA GOVERNANCE | COMPLIANCE MANAGEMENT

'Layered Approach' to address both Identity and Data Governance & Administration, and Compliance Management.

Complete transparencies on different layers of access across infrastructures, systems, databases, and applications.

Lower Total Cost of Ownership (TCO)

Modern, light-weight & flexible architecture



Integrated Identity + Data Governance

360° view of Enterprise Risk

Automated Deployment Tools & Wizards

Wizards & Tools

Deployment Manager

Community Cloud