(IN)SECURE

RSA CONFERENCE 2014

SPONSORED BY

QUALYS®

Welcome to (IN)SECURE Magazine special issue: RSA Conference 2014

To say that this year's RSA Conference was a large event is an understatement. A record number of more than 28,500 attendees experienced more than 410 sessions, keynotes, peer-to-peer sessions, track sessions, tutorials and seminars, which featured 604 speakers.

On top of that, spread over two expo floors, a total of 400 companies 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 allows 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

Distribution

Company index

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

The future of infosec: Securing the whole digital ecosystem

by Brian Honan

This year's RSA Conference USA was an interesting one for many reasons. Not only was it the biggest conference ever with a record number of attendees, but also in terms of the number of exhibitors showcasing their wares. There were over 500 speaking sessions with many other briefing talks at various vendor stands.

The recent controversy over allegations of the US National Security Agency paying RSA Security to introduce a backdoor into one of their products lay on the minds of many of the people attending.

Other allegations made by Edward Snowden about US government's mass surveillance, spying on friendly nations, and looking to undermine the security of the services and products we use on the Internet also cast a shadow.

The main message coming from many of the talks was about the need to better prepare for the eventuality of your organization suffering a security breach. Many talked about the need to develop the capabilities to better detect attacks, how to respond to attacks faster and more effectively, and how to share information with others so we can better deal with those attacking our systems. Indeed, my own talk was centered on "Disrupting the Progression of a Cyber Attack." It was a talk I gave with Dwayne Melançon, the CTO for Tripwire, and we focused on techniques and strategies for actively defending your network against a real-time cyber attack.

However, these subjects were not the ones that piqued my interest at this year's conference.

Having attended many RSA Conferences both in Europe and the US, what surprised me this year was the subtle shift in focus away from corporate security challenges to the security challenges facing individual consumers and users.

One of the keys areas that brought this focus to the consumer were the many talks about securing the Internet of Things (IoT). In particular, how we will need to develop strategies to secure these devices.

Last year we saw a Linux-based worm target the IoT. More recently we've seen attacks against consumer-based broadband routers with the TheMoon virus and in a separate incident where 300,000 routers were compromised in a DNS hijacking campaign. Given that many users still find it difficult to patch their PCs, imagine the challenges users, and indeed vendors, will face in patching the Internet of Things? Will we have a monthly patch Tuesday ritual where we patch all our wearable technology, our Internet-enabled kitchen appliances such as fridges, our cars, our embedded medical devices?

Another trend that caught my attention was the increase of the mobile malware threat. This is an issue that affects both enterprises and end consumers. Many do not have any security software on their devices, yet mobile phones and tablets are fast becoming the default way for people to surf the Internet, communicate with friends, and even buy things online or use near field communication (NFC) technologies.

The recent bugs discovered in SSL for iOS and Linux highlight the insecurity of the mobile platforms. Our devices are becoming more and more communicative too, the average smart device has at least five ways to connect to other devices, such as the mobile network, Wi-Fi, Bluetooth, Infra-red, and NFC technology. Who knows in what other ways our mobile devices will communicate in the future? Keeping all these channels secure all the time will be nearly impossible for most consumers.

Crypto currencies such as BitCoin were also the topic of many conversations in the speaker sessions and in the hallways. The general consensus was that crypto-currencies are here to stay and organizations should be prepared to use them. However, as we have witnessed in the past, criminals follow the money. We have already seen a number of criminal attacks against crypto currencies. A number of exchanges have been breached resulting in large financial losses and in some cases those exchanges going out of business. A number of viruses have been designed to target users' digital wallets and empty them of their contents. We have also seen botnets being used to mine crypto coins on behalf of the criminals running them.

The rise of ransomware use by criminals is another proof that criminals are switching to targeting individuals rather than concentrating their efforts on corporate targets. The recent Threat Assessment on Police Ransomware by Europol's European Cybercrime Centre shows that these attacks are a massive source of income for criminal gangs.

What this year's RSA Conference highlighted to me is that as our lives become more and more interconnected and dependent on the Internet we need to ensure we look at securing the whole digital ecosystem and not just concentrate on securing enterprises.

Without secure consumers and a secure Internet businesses will not be able to survive online by themselves. We need to work together to ensure security is built into all the services and products that we use and mechanisms are put in place to enable us to work and collaborate together when dealing with online threats.

Brian Honan is an independent security consultant based in Dublin, Ireland, and is the founder and head of IRISSCERT, Ireland's first CERT. He is a Special Advisor to the Europol Cybercrime Centre, an adjunct lecturer on Information Security in University College Dublin, and he sits on the Technical Advisory Board for a number of innovative information security companies.

He has addressed a number of major conferences, he wrote the book ISO 27001 in a Windows Environment and co-author of The Cloud Security Rules.

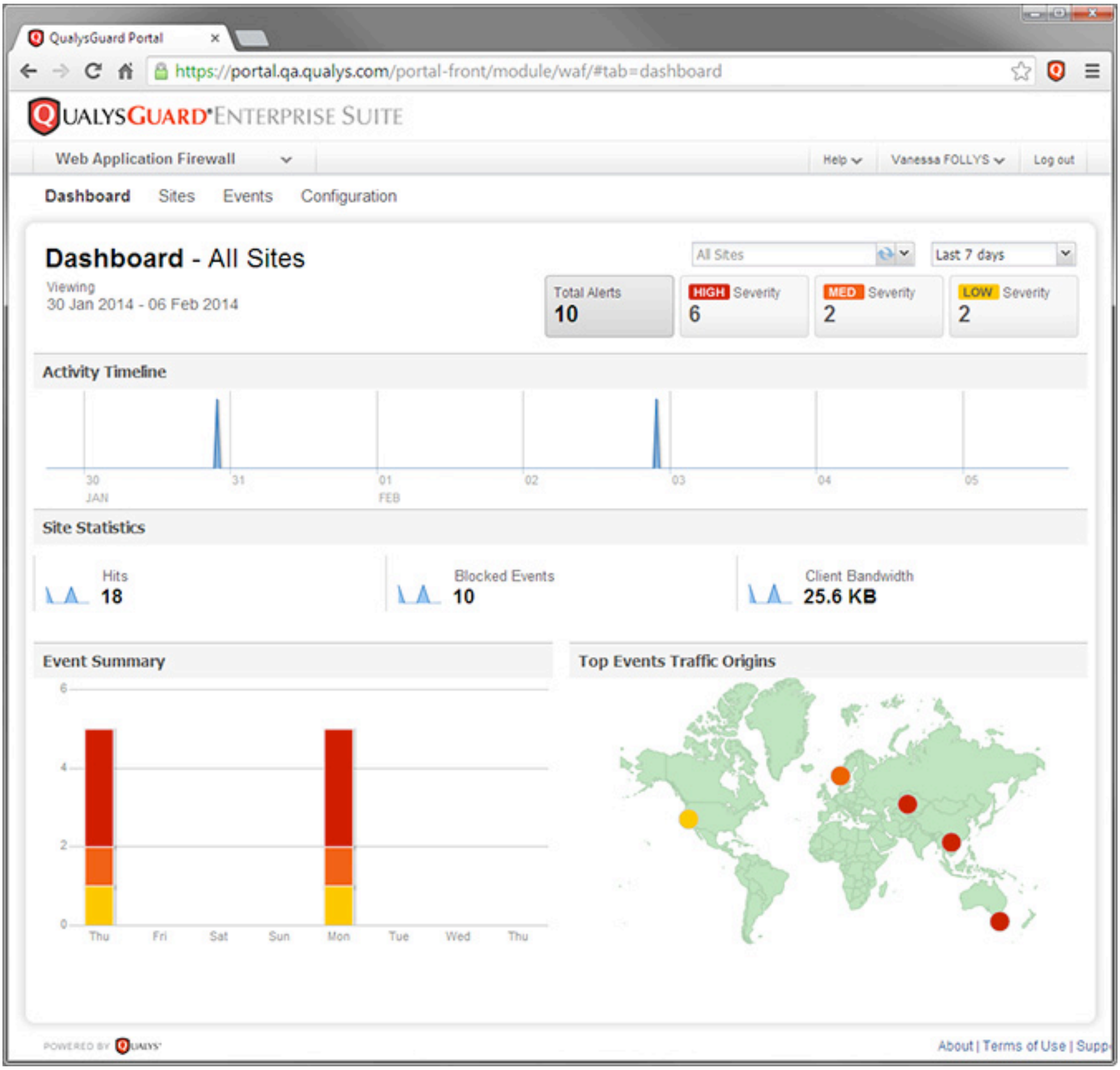
Qualys releases Web Application Firewall

Qualys announced the availability of its QualysGuard WAF service for web applications running in Amazon EC2 and on-premise. Deployed as a virtual image alongside web applications, the QualysGuard WAF can be set up and configured within minutes, enabling organizations to provide protection for their websites.

WAF technology shields websites by applying sets of rules to HTTP conversations to prevent them from being attacked, but the technology is typically costly and difficult to apply because the rules need to be updated often to cover application updates and to address changing threats.

The QualysGuard WAF cloud service provides rapid deployment of robust security for web applications with minimal cost of ownership, and it is constantly updated with new rules to keep up with application updates and newly emerging threats.

“Large organizations typically have thousands of web applications to protect, while smaller businesses don’t have the resources and IT staff to protect them,” said Philippe Courtot, chairman and CEO for Qualys. “The general availability our WAF service will offer customers the flexibility they need to protect their applications no matter where they reside and whether they have a few or thousands of them.”



https://portal.qa.qualys.com/portal-front/module/waf/#tab=dashboard

Dashboard - All Sites

Viewing
30 Jan 2014 - 06 Feb 2014

Total Alerts 10

HIGH Severity 6

MED Severity 2

LOW Severity 2

Site Statistics

Hits 18

Blocked Events 10

Client Bandwidth 25.6 KB

SANDBOX
BLUEBOX

wwpass
Security without back doors
Authentication without passwords
Privacy without compromises

ARBOR
FORTINET
NetIQ
beyondtrust
proofpoint
SilverSky
ORACLE
1600
NetIQ
KASPERSKY lab
RSACONFERENCE2014
AppRiver
Lieberman Software
Oracle
Proofpoint, Inc.
Raytheon
SilverSky
Wave Systems Corp.
SilverSky

EASYSOLUTIONS
Multi-Layer Fraud Protection
Safe Browsing
Fraud Intelligence
TOTALFRAUD

What people think about passwords, email snooping and personal data

Fortinet published new research that shows where Millennials and Gen-Xers stand in regards to passwords, online marketing practices, email snooping, and their personal data.

Based on findings from an independent US-based survey of 150 Gen X (ages 33-48) and 150 Millennials (ages 18-32) with a 50/50 male/female split, the survey revealed 41% of both Millennials and Gen-Xers never change their online password or only change it when prompted.

Of the respondents who signaled they are vigilant about changing their passwords, 16% (19% Millennial, 13% Gen-X) change them once a month, 30% (25% Millennial, 35% Gen-X) change them every three months and 9% (11% Millennial, 7% Gen-X) change them at least once a year.

When asked if they had a password to access their phone, 57% said they did, while 43% said they did not. Apparently, Gen-X is more trusting in this regard, with 49% saying they do not use a mobile device password, while a fewer number of Millennials (37%) admitted to not having a password on their device.

Of those who admitted to using a password on their mobile device, the most popular type by far was the simple 4-digit pin (numeric password), taking the top spot at 47%. Complex passwords, such as alphanumeric, letters and numbers, came in second with 26%. This was closely followed by pattern (i.e., triangle, square) at 21%. And in last place was biometric (i.e., facial recognition, fingerprint) at 5%.

40% of all respondents said they have a different password for every online account they use, 46% admit to having different passwords for at least a few of the sites they visit. 7% use different passwords for their most sensitive accounts and another 7% are using the same password for all accounts.

Network forensics platform for the 10 Gig world

nPulse Technologies announced the launch of its Cyclone Network Forensics Platform, which builds on full packet capture by adding advanced, line-rate extraction of crucial application layer security metadata and a flexible big data security analytics framework to index, search, analyze, and visualize network traffic and expeditiously reconstruct cyber attack kill chains.

By automating a comprehensive cycle of steps ensuring that all network traffic is captured and inspected for forensics and incident response activities, Cyclone provides the traffic visibility necessary to defeat attacks and reduce mean time to resolution for advanced network threats.

Protect your files from prying eyes.

EGNYTE®

Because the cloud is not enough.

Strong authentication for cloud apps from Duo Security

Duo Security is expanding their security platform to help customers protect access to their sensitive data residing in cloud-based applications, including Salesforce, Google Apps, Microsoft Office 365, and Box.

We certainly see the economic and management benefits of the cloud, but we're only going to take advantage of them if we can do so securely," said Mark Maher, Director of Corporate Infrastructure & Technology at New World Systems. "The enforcement of strong authentication empowers companies like ours to preserve control by fortifying access to company assets, no matter where they're hosted, on-premises or in the cloud. We use Duo Security to protect access to our VPN and Salesforce."

Duo Security's two-factor authentication platform is designed to integrate with an expansive range of applications, devices, and services, providing protection of user credentials. To address the evolving nature of hybrid IT models, Duo has expanded support to protect widely-utilized, cloud-based productivity applications and online storage services.

"To date, we've focused on providing customers with a two-factor authentication solution that is not only easy to use but also flexible enough to meet the ever-changing needs of organizations large and small," said Richard Li.

Free vulnerability management service for SMBs

Tripwire debuted Tripwire SecureScan, a comprehensive vulnerability management solution that requires no hardware or software to be installed and managed. Organizations of any size can use the service to discover detailed information about networked devices and find vulnerabilities in hardware and software applications that are used in cyberattacks. The solution discovers these vulnerabilities and then provides users with prioritized, in-depth information on how to fix these security weaknesses.

Enterprise crypto and authentication in one rackmount

Futurex announced the release of CryptoCube, a purpose-built, all-in-one rackmount enclosure for the secure encryption, decryption, authentication, and validation of sensitive data.

The CryptoCube system consists of a customized, multifactor authentication-secured rackmount enclosure containing a mix of Futurex Hardened Enterprise Security Platform solutions tailored specifically to the needs of each organization using it.

CONTINUOUS SECURITY
IN A UNIFIED SOLUTION
ASSET DISCOVERY
NETWORK SECURITY
WEB APP SECURITY
THREAT PROTECTION
COMPLIA MONITOR
WEB APP SECURITY
IT-GRC
VULNERABILITY MANAGEMENT

Microsoft Enhanced Mitigation Experience Toolkit (EMET)
Cloud Trust
QUALYS
Security Reimagined
XBOX ONE

FORGEROCK
Buildir ecu Relat ships
Acro e M ern
GEICO
McKESSON
sky
TriNet
FORGEROCK

FireEye

NetIQ
Identity-Powered Secur
Reduce Risk of Insider Attack with Identity Context

The DigiCert team at the conference.

Identify and fix vulnerabilities in your SSL certificates

DigiCert announced DigiCert Certificate Inspector, a tool designed to quickly find problems in certificate configuration and implementation, and provide real-time analysis of an organization's entire certificate landscape, including SSL termination endpoints.

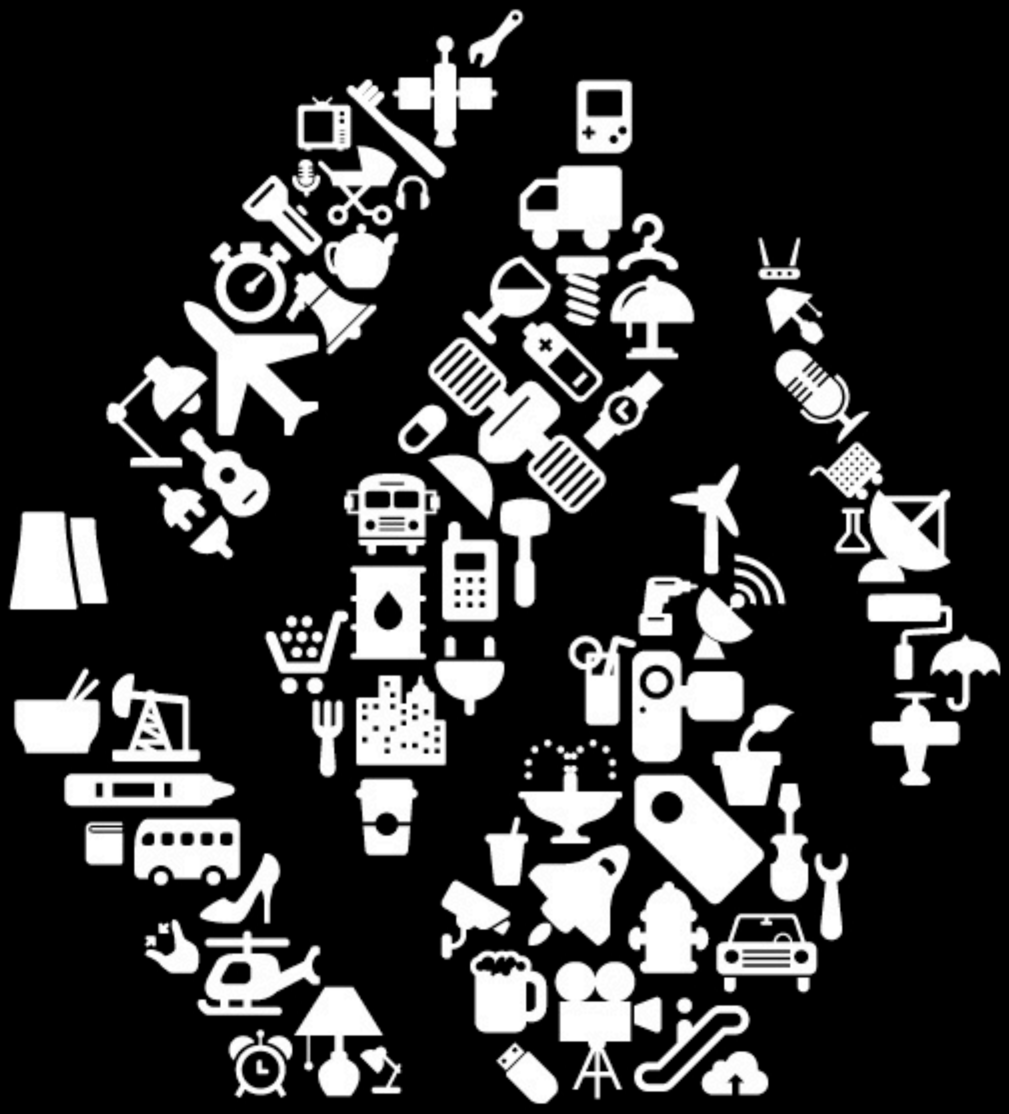
SSL/TLS certificates are a key defense against unwanted surveillance of online user activity. Yet, too often system administrators fail to properly configure certificates, unknowingly leaving open vulnerabilities.

Keeping up with the latest security best practices as well as monitoring certificates is a daunting task, particularly for enterprises managing thousands of certificates. Frequently, manual tracking processes are used, which introduce human error and result in downtime or unknown security vulnerabilities such as configuration with cipher suites vulnerable to CRIME, BEAST, BREACH or other attacks.

In other cases, departments outside of IT might deploy their own certificates, creating a blind spot for Administrators. This also can lead to configuration challenges that downgrade the effectiveness of the SSL certificates upon which organizations rely.

With Certificate Inspector, security professionals can discover forgotten, neglected or misconfigured certificates, and identify potential vulnerabilities, such as weak keys, problematic ciphers and expired certificates. For each potential threat detected, the tool provides a list of remediation activities.

Certificate Inspector scans the user's network detecting all certificates in use, inspects SSL configuration and implementation, and then displays the results in an intuitive and interactive dashboard.



DB Networks' virtual IDS stops advanced SQL injection attacks

DB Networks introduced the IDS-6300v intelligent security virtual appliance, a new solution based on the next-generation Core IDS platform introduced last year in DB Networks' IDS-6300 Core IDS hardware appliance.

Now, cloud providers and MSSPs can easily deliver new security SaaS offerings based on DB Networks' patented behavioral analysis technology for comprehensive SQL injection intrusion detection and defense.

Additionally, organizations operating virtualized data centers interested in protecting their core network can benefit from the cost savings delivered in IDS-6300v over hardware alternatives, while large enterprises can leverage its enhanced ease-of-management features.

The recent high-profile attacks on major retailers such as Target and the theft of millions of customers' private information serve as a strong reminder that database networks are highly susceptible to attacks. DB Networks' intelligent security virtual appliance delivers advanced and Zero-Day SQL injection attack detection. The IDS-6300v is the industry's first Core IDS as a virtual appliance that combines behavioral analysis and advanced continuous database monitoring that alerts of attacks and database network behavioral anomalies in real-time.

The solution, which enables security as a service offerings, also addresses specific compliance requirements within regulations such as PCI DSS, HIPAA, GLBA, and NIST spec 800-53.

Encryption management platform for protection in hybrid clouds

AFORE Solutions announced the addition of CloudLink SecureVM and CloudLink SecureFILE modules to the CloudLink encryption platform.

The additions build on the existing CloudLink SecureVSA and provide AFORE customers with flexibility to layer encryption at multiple points of the cloud computing stack with storage, virtual machine, file and application level solutions deployed and managed from a common framework.

CloudLink integration with hypervisor and cloud platforms enables IT personal to efficiently deploy security controls at all levels of the infrastructure. The net impact is better control, lower TCO and improved business agility to secure sensitive data and embrace the cloud with confidence.

ULTIMATE
LIGHTNING
WINNER

the Real World
cisco
Barracuda

tufin
The Goldilocks Zone
Insider Theft, Happening in Your Business

Network
Security
AUTOMATED

R·sam
Security Intelligence. Think Integrated.
IBM
1300
Check Point
SOFTWARE TECHNOLOGIES LTD.
EFINED
PROTECTION
OIN THE
ECURITY
EVOLUTION
RSACONFERENCE2014
Arbor Networks
Dell Inc.
Dell SecureWorks
Fortinet
Net Optics, Inc.
NXP Semiconductors
WatchGuard Technologies, Inc.
DELL
Attachmate

Egnyte appoints new CSO, unveils security roadmap

Egnyte formally introduced Kris Lahiri as the company's new CSO and unveiled his FY14 security roadmap, which details the company's plans to raise the global standard for secure file sharing in the enterprise.

Lahiri's plans include adding key security enhancements and integrations for secure deployment options, data privacy and industry standards.

Lahiri's 2014 security roadmap focuses on enhancements and integrations to provide Egnyte customers with secure access to 100 percent of their business files from any device, regardless of where those files physically reside.

"Egnyte is the only file-sharing solution built from the ground up to meet the needs of the enterprise," said Lahiri. "As the market evolves, so do the needs of our customers, and nothing is more vital to a business than the security of its most valuable asset - its business data. Combined with the varying industry standards in which businesses are required to comply, we understand how crucial it is to share our roadmap with our customers so they understand how Egnyte plans to meet all of their security needs now and into the future."

Identity relationship management market to exceed $50 billion by 2020

ForgeRock announced that the identity relationship management (IRM) market, focused on managing customer interactions across any device or environment, will exceed $50 billion by 2020.

This high growth market trajectory reflects the growing need for an effective IRM solution as CIOs shift investment from internal identity projects focused on "keeping things out" to massive external identity projects focused on increasing customer engagement and monetizing those opportunities.

Identity services must be in place regardless of sector — retail, finance, insurance, healthcare, government, cloud service, education — in order to extend business reach via social, mobile, cloud, and the Internet of Things.

According to Cisco, an estimated 8.7 billion things were connected to the Internet in 2012, expecting to grow to 50 billion Internet-connected things by 2020. ForgeRock estimates that every Internet-connected thing will require identity services in order to make real-time user access decisions based on context. As the Internet of Things (IoT) grows, ForgeRock expects an increase in the number of applications serving each device, driving an increase in identity revenue per device — approximately $50 billion in total opportunity.

OpenID Foundation launches the OpenID Connect Standard

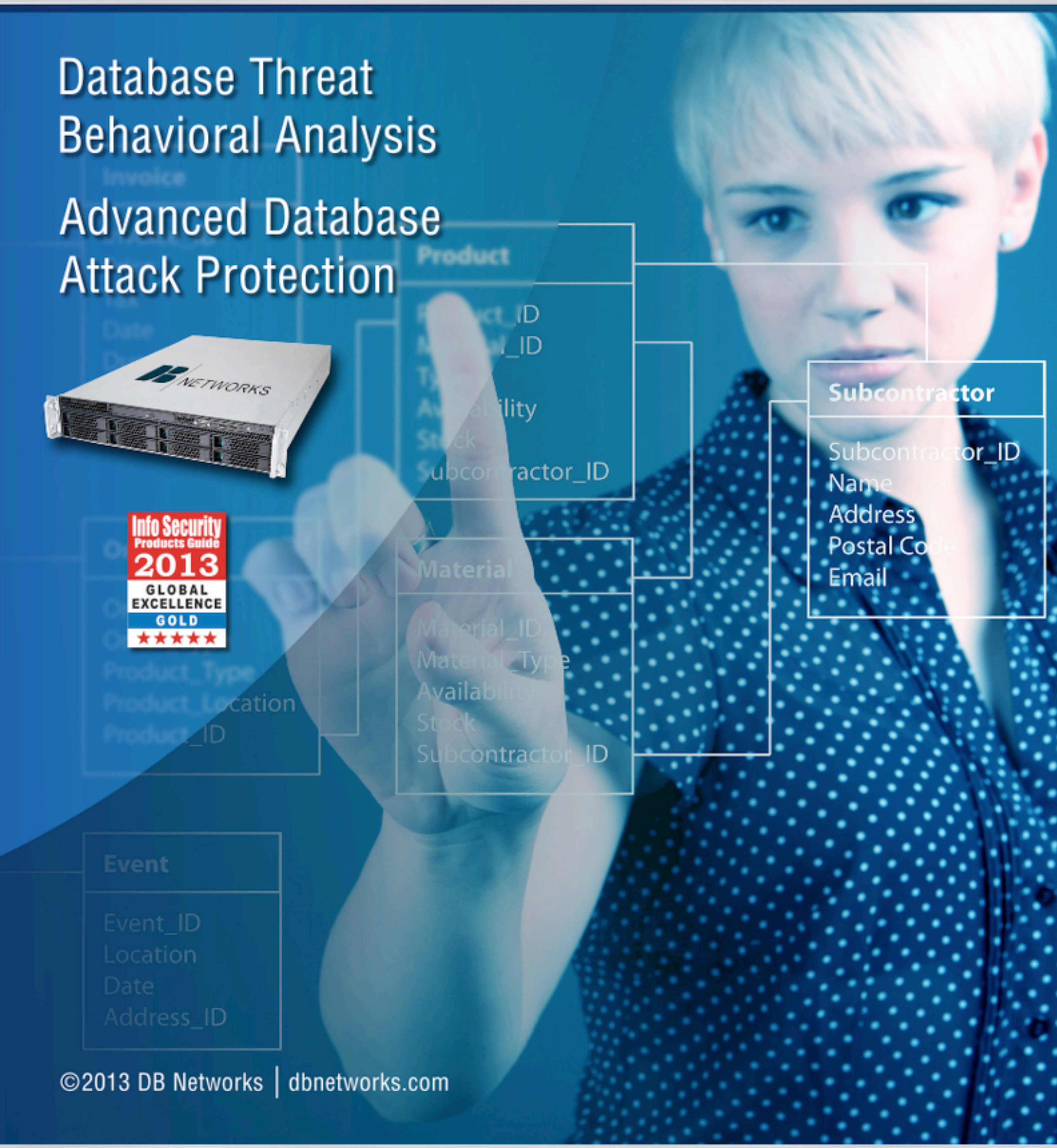
OpenID Connect is an efficient, straightforward way for applications to outsource the business of signing users in to specialist identity service operators, called Identity Providers (IdPs). Most importantly, applications still manage their relationships with their customers but outsource the expensive, high-risk business of identity verification to those better equipped to professionally manage it.

It has been implemented worldwide by Internet and mobile companies, including Google, Microsoft, Deutsche Telekom, salesforce.com, Ping Identity, Nomura Research Institute, mobile network operators, and other companies and organizations. It will be built into commercial products and implemented in open-source libraries for global deployment.

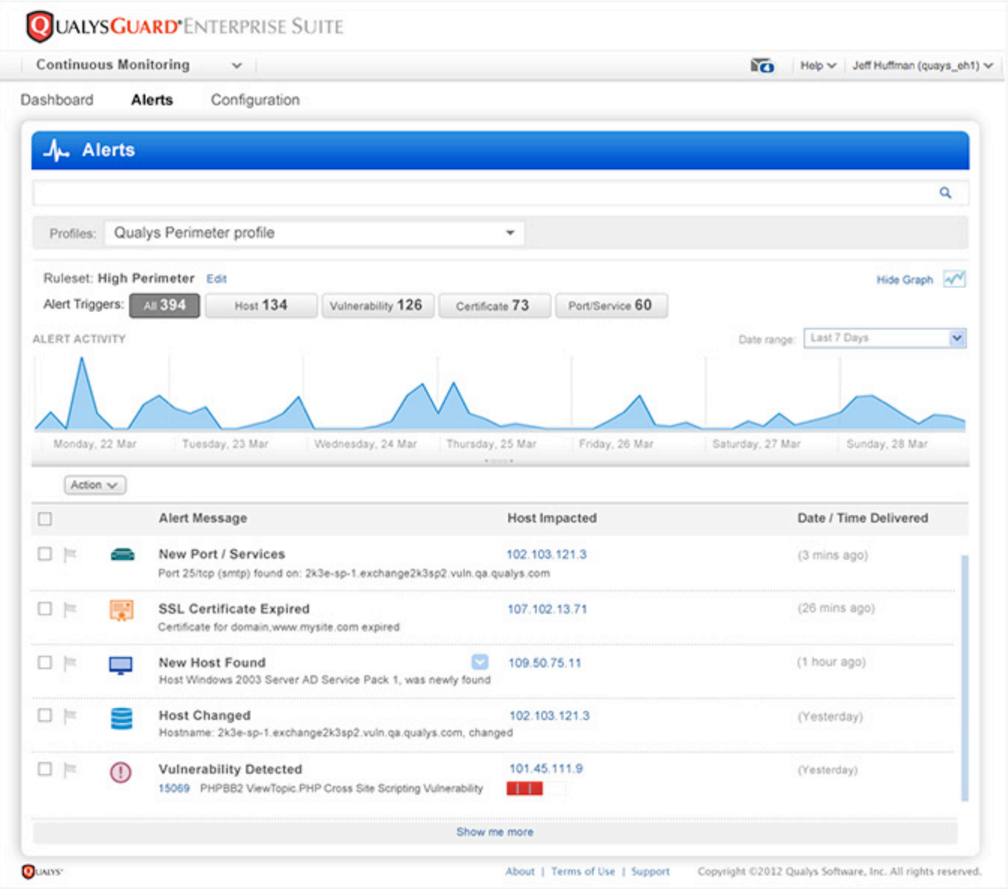
DB NETWORKS®

Database Threat Behavioral Analysis

Advanced Database Attack Protection



Info Security Products Guide 2013 GLOBAL EXCELLENCE GOLD ★★★★★



Profiles: Qualys Perimeter profile

Ruleset: High Perimeter Edit

Alert Triggers: All 394 | Host 134 | Vulnerability 126 | Certificate 73 | Port/Service 60

Date range: Last 7 Days

☐		Alert Message	Host Impacted	Date / Time Delivered
☐		**New Port / Services** Port 25/tcp (smtp) found on: 2k3e-sp-1.exchange2k3sp2.vuln.qa.qualys.com	102.103.121.3	(3 mins ago)
☐		**SSL Certificate Expired** Certificate for domain,www.mysite.com expired	107.102.13.71	(26 mins ago)
☐		**New Host Found** Host Windows 2003 Server AD Service Pack 1, was newly found	109.50.75.11	(1 hour ago)
☐		**Host Changed** Hostname: 2k3e-sp-1.exchange2k3sp2.vuln.qa.qualys.com, changed	102.103.121.3	(Yesterday)
☐		**Vulnerability Detected** 15069 PHPBB2 ViewTopic.PHP Cross Site Scripting Vulnerability	101.45.111.9	(Yesterday)

Qualys introduces Continuous Monitoring cloud service

Qualys introduced Continuous Monitoring, the most recent addition to its QualysGuard Cloud Platform.

This new offering gives organizations the ability to proactively identify threats and unexpected changes in Internet-facing devices within their DMZ, cloud-based environments, and web applications before they are breached by attackers.

It brings a new paradigm to vulnerability management, empowering customers to continuously monitor mission-critical assets throughout their perimeter and immediately get alerted to anomalies that could expose them to cyber attacks.

This new service allows companies to continuously monitor:

Hosts and devices exposed to the Internet – to see whenever systems appear, disappear, or are running unexpected operating systems.

Digital certificates – to track SSL certificates used on systems to know if they are weak or self-signed, and when they're due to expire.

Ports and services open on each system – to keep tabs on which network ports are open, which protocols are used, and whether they change over time.

Vulnerabilities on hosts or applications – to know when vulnerabilities appear (or reappear), whether they can be exploited, and if patches are available.

Applications installed on perimeter systems – to find out when application software gets installed or removed from these systems.

Enterprise-level UTM for home and small offices

WatchGuard Technologies announced the WatchGuard Firebox T10 UTM solution, a network security appliance that allows enterprises to extend powerful network security to SOHO environments.

It features WatchGuard's cloud-based RapidDeploy capability, which instantly self-configures and begins reporting back to the administrator's central console by simply plugging in the appliance.

FORGEROCK
Building Secure Relationships Across the Modern Web

RSA CONFERENCE SANDBOX
Identity Protection Management Data Services Attacks Authentication Enterprise Web Standards

CONTINUOUS SECURITY
IN A UNIFIED SOLUTION
ASSET DISCOVERY
NETWORK SECURITY
WEB APP SECURITY
THREAT PROTECTION
COMPLIANCE MONITORING
ASSET MANAGEMENT
VULNERABILITY MANAGEMENT
IT-GRC
WEB APP SECURITY
verizon
Top 4 Security Control
qualys.com/
HOST:
Philippe Courtot, Chairman
PARTICIPANT

digicert

EMC

McAfee expands Comprehensive Threat Protection

McAfee announced expanded capabilities to find, freeze, and fix advanced threats faster to win the fight against advanced and evasive targeted attacks.

The solution tightly binds and shares threat intelligence and workflows across endpoints, network and the cloud. It provides protection, performance, and operational savings that are not possible from point products, which aren't designed to optimize security and risk management as an IT function and carry the overhead of manual integrations.

Quickly identify and act on endpoint security issues

Promisec announced plans for Promisec Integrity, a series of cloud-based offerings to help small-to-medium enterprise organizations with endpoint security and remediation.

"Promisec Integrity is like a 'don't panic' button that can quickly provide peace of mind—and a course of action—for small-to-medium enterprises that must get ahead of the latest threats before they negatively impact corporate IP, operational efficiency and, ultimately, brand trust and profitability," said Dan Ross, CEO, Promisec.

New free online software security training courses

SAFECode, a non-profit organization working to increase trust in technology products and services through the advancement of effective software assurance methods, announced that it has released new software security training courses as part of its online Security Engineering Training by SAFECode program.

Security Engineering Training by SAFECode is an online community resource offering free security training courses delivered via on-demand webcasts. Covering issues from preventing SQL injection to avoiding cross site request forgery, the courses are designed to be used as building blocks for those looking to create an in-house training program for their product development teams, as well as individuals interested in enhancing their skills.

Android, iOS solution reveals data-leaking apps

Unlike traditional mobile security apps, which utilize a database of known malicious apps to screen for viruses and malware, viaProtect monitors all apps for mobile risks. For instance, viaProtect can detect if an app handles your personal data insecurely by transmitting it unencrypted or to servers located overseas. **viaForensics** estimates that as many as 75 percent of apps are "leaky", or insecure.

viaProtect gathers mobile forensic, system, network, security and sensor data from devices, then utilizes statistical analysis and risk indicators to detect suspicious events or behavior.

Nearly half of companies assume they have been compromised

A majority of organizations are operating under the assumption that their network has already been compromised, or will be, according to a survey conducted by the **SANS Institute** on behalf of **Guidance Software**.

SANS surveyed 948 IT Security professionals in the United States to determine how they monitor, assess, protect and investigate their endpoints, including servers.

The survey results demonstrated that more and more attacks are bypassing perimeter security, despite the fact that the respondents do not consider the attacks to be sophisticated. Survey respondents indicated the desire for more visibility into more types of data and processes across organizational endpoints as intruders evade perimeter defenses.

?
23
27
00
232700
232700

Cyber crooks will go after medical records next

As security firms and law enforcement agencies continue to cooperate and successfully take down botnets, cyber crooks will be forced to look for new and more lucrative targets, and especially ones that are poorly secured.

In a panel held at RSA Conference, the **Microsoft/ Agari** team behind the Citadel botnet takedown said that these new targets will likely be in the healthcare industry.

After explaining just how they went about effecting the takedown, they explained the reasoning behind their belief that healthcare IT systems and hospital databases are next in line for data breaches. Agari CEO Patrick Peterson shared that the price of medical records belonging to a single person might fetch around $60, while a single credit card record is worth a couple of dollars in the underground markets.

He also pointed out that among the industries targeted so far, financial organizations and social networks have worked hard on protecting their customers, and have made cybercriminals' attempts more difficult and, therefore, more costly. On the other hand, the majority of the healthcare industry has not followed suit.

In addition to all this, medical records give crooks much valuable information about a target that can be misused for mounting effective social engineering attacks, noted Richard Boscovich, assistant general counsel with the Microsoft Digital Crimes Unit.

44% of companies don't have a cloud app policy in place

After interviewing 120 RSA Conference attendees, **Netskope** announced the results of the survey on information security professionals' use of cloud apps.

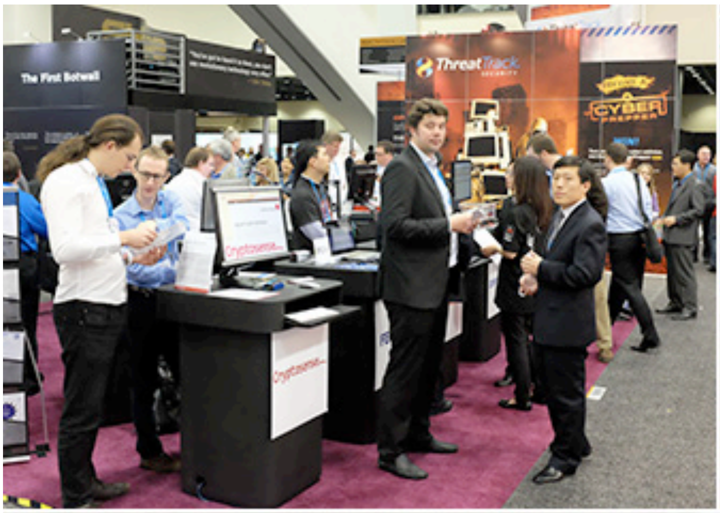
Despite widespread adoption of cloud apps in the enterprise, most IT security professionals are either unaware of their company's cloud app policy or don't have one. In the absence of cloud app policies, more than two-thirds of attendees surveyed said they would consider their company's privacy policy before downloading an app.

As cloud apps proliferate in the enterprise, the security and privacy risks associated with use of these apps at work is on the rise. According to the recent Netskope Cloud Report, the typical enterprise is using 397 apps, or as much as 10 times the number that IT typically has within its purview. Although enterprises have more cloud apps in use by employees than ever before, 44 percent of those surveyed said their company doesn't have a cloud app policy in place. Furthermore, 17 percent of employees are unaware if their company has a policy.

Webroot delivers APT protection for enterprises

Webroot announced the release of BrightCloud Security Services and BreachLogic Endpoint Agent, two cloud-based security offerings designed to help enterprises address the explosive growth and increasing sophistication of online threats, particularly targeted attacks such as spear phishing and APTs.

BrightCloud Security Services redefine online threat intelligence. The suite of cloud-based services, powered by a self-learning threat analysis platform that continuously scans the internet, is designed to help enterprises and OEM technology partners strengthen their security technology with accurate and actionable threat intelligence. The enhanced suite includes a new File Reputation Service and an enriched contextual database that correlates previously disparate security data points.


The First Botwall
ThreatTrack SECURITY
CYBER

QUALYS CONTINUOUS SECURITY
3000
Microsoft
FireEye
UE COAT
QUALYSGUARD® CLOUD PLATFORM
Continuous Security in a Unified Solution
Theater Schedule
ca

intel Security
JUNIPER NETWORKS
DECEPTION FORCE
cisco

algosec
Automated Security Policy Management for Your Data Center and Network
NEXT DEMO

Free tool helps fend off most cyber attacks

Qualys announced that it has collaborated with the SANS Institute and the Council on CyberSecurity to release a new free tool to help organizations implement the Top 4 Critical Security Controls to fend off attacks.

The new tool helps organizations quickly determine if the PCs in their environments have properly implemented the Top 4 Critical Security Controls, which the Council on CyberSecurity estimates can help companies prevent 85% of cyber-attacks.

"The Qualys Top 4 tool is an extremely elegant and effective solution that helps both small and large businesses determine how resilient they are to today's advanced threats," said Jonathan Trull, CISO for the State of Colorado. "This is exactly the type of public-private partnership our country needs to address the cyber attacks threatening our economy and critical infrastructure."

Built on the QualysGuard Cloud Platform, the new Top 4 cloud service helps businesses easily and quickly identify whether Windows PCs in their environments have implemented the Top 4 controls for:

1. *Application Whitelisting* – only allowing approved software to run.
2. *Application Patching* – keeping applications, plug-ins and other software up to date.
3. *OS Patching* – keeping operating systems current with the latest fixes.
4. *Minimizing Administrative Privileges* – preventing malicious software from making silent changes.

IT Administrators can then use the reports from the free tool to track endpoints that are not in compliance and apply the necessary measures to make them more resilient to attacks.

RSA Conference attendees ambivalent about NSA tactics

Thycotic Software announced the results of a survey of 341 RSA Conference 2014 attendees, which found that 48% of pollees feel the NSA overstepped its boundaries in its surveillance of US citizens.

At the same time, three quarters (75%) of respondents, regardless of their stance on the NSA, think those who boycotted RSA Conference this year have a right to their opinion, and 9% had even contemplated joining them. Only 17% say those who boycotted RSA are attention seekers.

The survey also uncovered widespread belief that abuse of privileged access occurs within attendees' organizations. Only 19% of respondents are confident that such access, often referred to as the "keys to the kingdom," is used properly. In what may signal a resignation to this reality, roughly one in five (19%) RSA attendees indicate that they would still hire Edward Snowden, given the opportunity.

Other key findings from the survey include:

- Of the 52% of respondents who did not indicate that the NSA overstepped its bounds, 21% believe that the government needs to be aware of citizens' communications data in order to better protect them from terrorist activity, and 31% say they are conflicted about the issue, and that while they have nothing to hide, they are concerned about a loss of privacy.
- Alternatively, 48% of respondents unequivocally say the NSA did overstep its bounds in its surveillance of US citizens.
- 61% of respondents acknowledge that they either know that employees within their company have abused privileged access (24%) or that it is likely that they have (37%). Another 20% are unsure if this has happened.

Unfortunately, the survey doesn't say whether the pollees were US citizens or not.

WE NEED TOMORROW'S TECHNOLOGY
TODAY.
IN FACT, WE NEEDED IT YESTERDAY.

At NetIQ, we make your challenge our mission.

In today's connected world, your business users are always looking for faster, better ways of working and solving business problems. Unfortunately, the solutions they find can often add complexity and risk to your environment. At NetIQ, we understand your unique needs and how you can secure, manage and measure the services your business is delivering. The result? Value you can deliver at the speed your business demands.

Turn challenge into opportunity.
www.netiq.com/company

NetIQ.