SC MAGAZINE

AWARDS 2014

Honored in the U.S.

Feb. 25, 2014 • San Francisco

Cyber risk at an all-time high

Only recently did we hear about "The Mask," an advanced persistent threat (APT) which, when identified by Kaspersky Lab researchers, was said to be the chosen tool behind a seven-year-old cyber espionage campaign targeting government institutions, private equity firms, energy companies and many others in the U.S., U.K. and Morocco. Because of the highly skilled operational procedures used managing it, researchers believe it is state-sponsored.

Beyond APTs, data breaches – like those hitting Target and Neiman Marcus – have led their shoppers to experience more than just the mere theft of their credit card and ATM numbers. Many of the millions victimized by the breach had to deal with subsequent problems of identity fraud and, in some cases, account takeovers, according to some researchers.

And, how can we review problems plaguing information security and privacy pros without mention of the National Security Agency/Snowden happenings that came to the fore this last year. Revealing just how far government monitoring extends, information leaked from files that Edward Snowden pinched before leaving his contract position at the NSA shows evidence of the federal government keeping terabytes of metadata on its citizens, as well as creating backdoors in encryption tools and much more.

When it comes to data protection and risk management planning, information security pros like you must be aware of a host of issues. As you shore up your organizations' security controls to ensure they focus on your organization's most critical data – where it's stored, where it flows, who has access to it and more – you must do this while competing with other departments for dollars. And, at the same time, you must navigate a political landscape that requires a champion for security whose business acumen is just as well-honed as your technical prowess.

There's a tremendous amount of work to do as an IT security leader. Constantly evolving risk management plans, strengthening policies, deploying the right technologies to support these endeavors, educating colleagues and bosses alike…the list goes on. And, I'm betting, that's a main reason why security pros like you find the passion and dedication to take it on every day. That list and all the efforts that back it up is just one reason why my staff and I are honored to celebrate you, our industry's leading lights, for everything that you contribute to keep this community of curious, intelligent and devoted professionals advancing.

– *Illena Armstrong, VP, editorial,* SC Magazine

SC MAGAZINE AWARDS 2014 Honored in the U.S.

Contents

Reader Trust Awards

Excellence Awards

Professional Awards

EDITORIAL
VP, EDITORIAL Illena Armstrong
ASSOCIATE EDITOR Teri Robinson
MANAGING EDITOR Greg Masters
ONLINE EDITOR Marcos Colón
REPORTER Danielle Walker
REPORTER Adam Greenberg

2014 SC AWARDS U.S.
EVENTS DIRECTOR Natasha Mulla
EVENTS MANAGER Anthony Curry
ASSOCIATE EVENTS MANAGER Maggie Keller

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
PRODUCTION MANAGER Krassi Varbanov

U.S. SALES
VP, SALES David Steifman (646) 638-6008
REGIONAL SALES DIRECTOR Mike Shemesh (646) 638-6016
WEST COAST SALES DIRECTOR Matthew Allington (415) 346-6460
EVENT SALES DIRECTOR Mike Alessie (646) 638-6002
ACCOUNT MANAGER Samantha Amoroso (646) 638-6021

SALES/EDITORIAL ASSISTANT Ashley Carman (646) 638-6104
ACCOUNT EXECUTIVE, LICENSING AND REPRINTS Elton Wong (646) 638-6101

MANAGEMENT
CEO, HAYMARKET MEDIA Lee Maniscalco
EXECUTIVE VP Tony Keefe
COO John Crewe

2014 SC Awards U.S.

The Judges

CO-CHAIR

Illena Armstrong
VP, editorial,
SC Magazine

CO-CHAIR

Mark Weatherford
principal,
The Chertoff Group

Erik Avakian
CISO,
state of Pennsylvania

Rebecca Gurley Bace
president/CEO,
Infidel

James Beeson
CISO,
GE Capital Americas

Deven Bhatt
VP & CISO,
WEX

Dennis Brixius
VP & CSO,
McGraw Hill
Financial

Christopher Burgess
CEO & president,
Prevendra

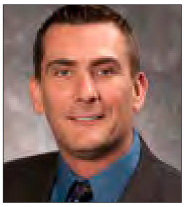
Miki Calero
CISO, state of Ohio -
Public Safety

Chris Camacho
senior vice president
– global information
security, Bank of
America

Jaime Chanaga
president,
The CSO Board

Chris Christianson
assistant VP of network services for one
of the nation's largest
credit unions

Dave Cullinane
VP of global security
and privacy, Catalina
Marketing



Bill Dennings
CISO, Nike

Cris Ewell
CISO,
Seattle Children's

Michael Fabrico
employed by world's
largest financial
exchange company

Stephen Fridakis
CISO,
United Nations FAO

Ira Greenstein
CISO, Maryland
State Retirement and
Pension System

John Johnson
global security
strategist, John Deere

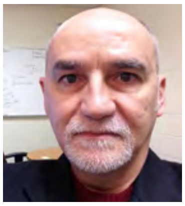
William Malik
principal,
Malik Consulting

Jim Maloney
CISO, Mercury
Payment Systems

Randy Marchany
CSO, Virginia Tech

Richard Marshall
chairman of the board
and CEO, Secure
Exchange Technology
Innovations

Theresa Masse
CISO, state of
Oregon



Scott Pearce
CISO, Fredrick
Country Government

Kris Rowley
information security
officer, state of
Vermont

Randolph (Randy) Sanovic
owner,
RNS Consulting

Steve Santorelli
manager of outreach,
Team Cymru

Sandra Sargent
senior operations
officer, World Bank

Alex Tosheff
CISO, Paypal

A. Spencer Wilcox
managing security
strategist and special
assistant to the CSO,
Exelon Corporation

Not pictured

Greg Hughes
VP and information
security officer,
Fiserv Digital
Channels

Jonathan Kaplan
director of information security, San
Francisco International Airport

The Sponsors

SC Magazine would like to thank all of our sponsors for their generous support of the 2014 SC Awards U.S. Their involvement has made this event possible, which helps raise professional standards in the information security industry worldwide.

Check Point Software Technologies

Check Point Software Technologies provides protection against threats, reduces security complexity and lowers total cost of ownership.

CloudPassage

A leading cloud infrastructure security provider and creator of Halo, a security platform purpose-built for cloud environments.

Entrust

A trusted provider of identity-based security solutions, Entrust secures governments, enterprises and financial institutions.

Exelis

Exelis is a defense and aerospace company providing mission-critical solutions to the U.S. military and its allies.

ForeScout

ForeScout delivers pervasive network security by continuously monitoring and mitigating security exposures and cyber attacks.

Halon Security

Halon Security is a technology leader of email security, load balancers and firewalls.

InfoSec Institute

Provides information security training to those seeking the most effective IT methods for today's business environments.

ISACA

A nonprofit, global association that develops and delivers industry-leading certifications, education and resources.

Kaspersky Lab

An international group operating in 200 countries, it is one of the world's leading endpoint security vendors.

MSLGROUP

MSLGROUP is one of the world's largest public relations, strategic communications and engagement firms.

Norse

Norse is a leading innovator of live threat intelligence solutions that enable organizations to identify and defend against cyber threats.

Northrop Grumman

A leading security company providing products and solutions to government and commercial customers worldwide.

Qualys

A leading provider of cloud security and compliance solutions with more than 6,000 customers in more than 100 countries.

Radware

A global leader of application delivery and security solutions for virtual and cloud data centers.

RSA

RSA, the Security Division of EMC, is a leading provider of enterprise security solutions.

Security University

A leading provider of cyber security education, information assurance training and certifications for IT and security professionals.

Splunk

Splunk software collects, indexes and harnesses the machine-generated Big Data coming from the devices that power business.

West Coast Labs

A test lab and technical consultancy specialising in the independent validation of information security products.

Welcome from the co-chairman

Reflecting back on 2013 I'm reminded of Sir Winston Churchill's statement that, "The farther back you can look, the farther forward you are likely to see." While I often say that the security issues we worried about a year ago are not the same things we worry about today, much of what happened in the past 12 months is symbolic of our future in the security business.

Data breaches in the retail industry, growing concerns about industrial control system vulnerabilities, the exploding Internet of Everything, and even the black swan event called the 'Snowden Effect' are having a dramatic impact on the security product and service industry. Nate Silver said that "Caesar recognized the omens, he just didn't believe they applied to him" and I think we're finally seeing a shift in businesses around the globe as they realize that maybe the security-omens do apply. Because our customers live in a world of imperfect choices, that means opportunity for us to help them find the best solutions.

What distinguishes most of the companies in this room tonight is an orientation toward action and your ability to look farther in space and shorter in time. That gives you a 'present at the creation' opportunity to build the kind of new security products the world needs for a more secure Internet. Elegance and intelligence are far better than brute force and ignorance and through your ingenuity and innovation, you are developing marvelous technologies that will make the Internet a safer place.

Someone once said that you've got to be an optimist to be in the security business. The SC Awards, and each of you here tonight, reflect that kind of optimism. Congratulations.

– Mark Weatherford
co-chairman, 2014 SC Awards U.S.;
principal, The Chertoff Group

Reader Trust Award

BEST ADVANCED PERSISTENT THREAT (APT) PROTECTION

WINNER

Websense for Websense TRITON Enterprise

Advanced persistent threats (APTs) are changing the security landscape and striking fear into the security professional's heart with each headline-grabbing targeted attack, data theft success and spear-phish. Signature-based defenses only detect 30 to 50 percent of known threats. These defenses are also generally focused on inbound-only threat protection, without considering possible data theft after intrusion. Websense TRITON Enterprise combines advanced threat detection for web and email traffic with full DLP capabilities for data-in-motion and at rest. One unified solution provides complete web, email and data security. TRITON Enterprise uses Websense ACE (Advanced Classification Engine) which analyze web and email traffic in real time with 10,000-plus analytics and composite risk scoring for signature-less threat identification. TRITON's inline real-time defenses cover the multiple stages of advanced threats for inbound and outbound traffic. This protects data in motion through web and email channels, as well as data at rest on servers and endpoints.

TRITON Enterprise differs significantly with advanced malware protection. It protects against malicious scripts and zero-day threats that circumvent anti-virus products. It also analyzes web traffic in real time, categorizing dynamic web content/threats to detect advanced payloads, exploited documents, mobile malware protection and much more. It also examines real-time content and security classifications for HTTPS and social websites, plus full webpage threat analysis for active scripts and malicious code. It extends use policies for social websites, which cannot be accurately classified by URL filtering.

Finalists 2014

- Check Point Software Technologies for Check Point Threat Prevention
- McAfee for McAfee Advanced Threat Defense
- Palo Alto Networks for WildFire
- Sourcefire for Sourcefire Advanced Malware Protection (AMP)
- Websense for Websense TRITON Enterprise

Reader Trust Award

BEST CLOUD COMPUTING SECURITY SOLUTION

WINNER

Juniper Networks for Juniper Firefly Host
(formerly vGW Virtual Gateway)

Organizations see security as an impediment to virtualizing. Further, the process of converting physical servers to VMs renders traditional security devices, like firewalls and IDS/IPS sensors, effectively "blind" to the new inter-VM traffic patterns. That's why a new level of visibility and granular per-VM-security is required for firms to meet internal and, in some cases, regulatory compliance. Because legacy security regimens and current virtualization management tools do not provide this functionality, a purpose-built solution is required. And in this area, Juniper is a pioneer – having been first to deliver zone synchronization between physical firewalls and those specific to virtualization. With Firefly Host, organizations have the benefit of virtualization security that is automated, dynamic and as scalable as the virtualized data center. Firefly Host lets those stakeholders who have delayed adopting virtualization bridge the confidence gap toward implementing secure cloud computing environments.

Firefly Host provides organizations with necessary firewall protections without performance trade-offs. This is due to its use of VMware Fast Path APIs that create an entire enforcement and packet processing firewall in the hypervisor kernel, separate connection tables for enhanced firewall processing, and patent-pending firewall rule base design that allows distribution of workload to virtual firewall instances and reduces the number of rules processed for VMs. Traditional anti-virus approaches deployed within virtualized environments are extremely punitive on CPU and RAM for guest VMs, using up far too much of these resources and requiring organizations to buy more VM hosting hardware to support additional protections.

Finalists 2014

- Check Point Software Technologies for Check Point Virtual Appliance for AWS
- Juniper Networks for Juniper Firefly Host (formerly vGW Virtual Gateway)
- Palo Alto Networks for VM-Series
- Rapid7 for Rapid7 UserInsight
- Trend Micro for Deep Security
- Zscaler for Zscaler Direct-to-Cloud Network

Reader Trust Award

BEST COMPUTER FORENSIC SOLUTION

WINNER

Guidance Software for EnCase Forensic

Guidance Software's EnCase software solution is a powerful, judicially accepted platform that provides the foundation for corporations, government agencies and law enforcement to conduct thorough and effective digital investigations of any kind, including intellectual property theft, incident response, compliance auditing and responding to e-discovery requests – all while maintaining the forensic integrity of the data. It includes the EnCase Enterprise software platform, which can support the EnCase Cybersecurity and EnCase eDiscovery applications. The product line also includes EnCase Forensic and EnCase Portable. EnCase allows customers to conduct more complete investigations with additional integration with a cloud-based eDiscovery platform, as well as security information and event managers (SIEM) for automated incident response.

The EnCase platform and applications address the requirements of an extremely broad range of users, including security specialists, investigators, computer incident-response teams and litigation specialists. It delivers everything needed to immediately and thoroughly search, collect, preserve and analyze data from servers, workstations, mobile devices and cloud-based data sources. With EnCase, users can be confident in their ability to complete a comprehensive analysis of whatever evidence they may encounter. The solution has the ability to customize how it functions, adding capabilities to the product to meet specific needs. For example, EnCase App Central offers more than 65 EnScripts or apps that allow users to add functionality and increase productivity.

EnCase allows for the automation of repeatable processes associated with the acquisition, analysis and reporting of a forensic investigation, eliminating redundant manual work.

Finalists 2014

- AccessData for Forensic Toolkit
- Cyber Security Technologies for P2P Marshal
- Guidance Software for EnCase Forensic
- Lancope for Lancope's StealthWatch System
- RSA, the Security Division of EMC, for RSA Security Analytics

Reader Trust Award

BEST DATA LEAKAGE PREVENTION (DLP) SOLUTION

WINNER

RSA, the Security Division of EMC, for RSA DLP

RSA DLP helps organizations gain visibility into risk and prevent the loss of sensitive data from accidents, malicious insiders and external attackers. RSA DLP discovers and monitors the location and flow of sensitive data – including regulated data or corporate intellectual property – across the infrastructure, including cloud, virtual and mobile devices. It can alert and educate end-users in real-time and enforce controls, such as encryption, quarantine, block and notify, to prevent the loss of sensitive data through email, web, PCs, smartphones, iPads, virtual desktops and more. Protocol- and port-agnostic, RSA DLP can see all network traffic, including traffic sent through non-standard ports, and with a web-based management console it allows organizations to set up a single DLP policy to protect sensitive data across the network, endpoints (connected or disconnected, including mobile) and datacenter, with centralized incident management for complete visibility into risk.

RSA DLP is port-agnostic and can analyze traffic from all network layers. It offers customizable workflows for incident management and investigations. RSA DLP can also be extended (with add-on modules) into GRC use cases for managing risk, audits, etc. Other unique differentiators include support for virtual desktops, virtual applications, hybrid cloud and private cloud; support for Macs, iOS, Android and Windows mobile; support for scanning public cloud-based repositories, including SharePoint Online; and an advanced analytical and classification engine for identifying intellectual property. Its ecosystem of technology partners includes Microsoft, VMware, Cisco, Citrix, VCE, EMC, Symantec and McAfee. Plus. it offers native encryption functionality and open APIs for partners.

Finalists 2014

- DeviceLock for DeviceLock Endpoint DLP Suite
- RSA, the Security Division of EMC, for RSA DLP
- Safetica Technologies for Safetica 5
- WatchDox for WatchDox
- Websense for Websense Data Security Suite

Reader Trust Award

BEST DATABASE SECURITY SOLUTION

WINNER

Check Point Software Technologies for Check Point 13500 Appliance

The 13500 Appliance protects against a wide spectrum of cyber attacks while meeting the growing demand for bandwidth and network performance. It delivers blazing-fast security with 23.6 Gbps firewall and up to 5.7 Gbps IPS using real-world SecurityPower Benchmark traffic mix and policy. In industry-standards-based performance tests, it achieves up to 77 Gbps of firewall, 17 Gbps of VPN throughput and up to 28 million concurrent connections. Four pre-defined security packages enable consolidation of vital security functions for next-generation firewall, threat prevention, data protection and secure web gateway, and enables hardware consolidation supporting up to 250 virtual systems. Extensive hardware features support a wide range of network options, and integrated onsite and remote management tools ease operations. Network expansion slots allow for numerous network options offering scalability, flexibility and high availability. The 13500 Appliance is available in two configurations: one fully flexible and the other pre-defined.

The tool integrates advanced, centralized management tools and includes the most updated IPS signatures available. It does not compromise security for performance, delivering both industry-leading firewall and IPS throughput plus optimal performance leveraging Check Point's advanced SecureXL, CoreXL and ClusterXL technologies to secure even the most demanding environments.

The offering includes integrated, centralized security management and is based on the Gaia OS which supports the latest networking standards and dynamic routing protocols, including IPv6. Automatic software updates increase operational efficiency and ease the management burden.

Finalists 2014

- Check Point Software Technologies for Check Point 13500 Appliance
- DB Networks for DB Networks IDS-6300 Core IDS
- McAfee for McAfee Database Security Suite for Databases
- Netwrix for Netwrix Auditor for SQL Server

Reader Trust Award

BEST EMAIL SECURITY SOLUTION

WINNER

Proofpoint for Proofpoint Enterprise Protection / Proofpoint Enterprise Privacy

Heightened awareness of data loss risks – highlighted by public breaches of media and government data – has increased enterprise concerns around email content management. This, paired with the increasingly complex regulatory environment and the rise of malicious and hard-to-detect email threats such as spear phishing and targeted attacks, which are at the root of many high-profile breaches, is driving the need for email security solutions. The evolving threat landscape is motivating the demand for both inbound and outbound email security solutions. Proofpoint Enterprise addresses this market with a solution that delivers unified inbound/outbound email security, data loss prevention and email encryption features. Proofpoint offers all gateway email security delivery models – SaaS, on-premises and software – as well as hybrid deployments. The solution is designed to meet the security and performance demands of even the largest enterprises. Proofpoint provides superior spam effectiveness (typically 99.8 percent or higher). Proofpoint makes it easy for customers to manage inbound email and outbound policies for both email and HTTP, the two most critical data loss vectors, from one location. Accurate content analysis, a wide variety of dispositions, support for multiple routes/channels and the ability to enforce different policies at global, group and individual levels make for a powerful, flexible system. Proofpoint's based management interface, paired with the integrated, policy-based encryption, ease-of-use and simple SaaS-based key management optimized for mobile devices, make the solutions attractive for administrators and users.

These capabilities work across enterprises devices meeting the needs of modern companies.

Finalists 2014

- Barracuda Networks for Barracuda Email Security Service
- McAfee for McAfee Email Protection
- Proofpoint for Proofpoint Enterprise Protection / Proofpoint Enterprise Privacy
- Trend Micro for ScanMail
- Websense for Websense Email Security Gateway Anywhere

Reader Trust Award

BEST FRAUD PREVENTION SOLUTION

WINNER

Entrust for Entrust TransactionGuard

A proven solution deployed in banks and government services around the globe, Entrust TransactionGuard is a zero-touch fraud detection solution that provides real-time monitoring of transactions to thwart today's most serious online threats without impacting business application or the user's experience. It requires no direct integration to banking applications or software on user devices, and includes an out-of-the-box library of behavior pattern baselines and supports easily customizable rules. It captures all transactional data, not just a subset, and includes "front door" device-profiling and IP host-reputation monitoring, as well as in-session transaction and web access patterns with automatic behavioral analysis. Should a session's risk score reach a certain threshold, the solution can either suspend, block or ask the user for additional authentication. Its proven engine helps identify emerging threats and captures transaction history for forensic fraud detection and post-transaction analysis.

Entrust TransactionGuard transparently monitors and profiles user behavior to identify anomalies, automatically learning what is normal for that user, and then calculates the risk associated with a particular transaction – all seamlessly and in real time. In addition, Entrust TransactionGuard performs both web session behavior profiling and user behavior profiling to provide financial organizations with comprehensive fraud detection.

Entrust's affordable real-time fraud detection solution enables organizations to reduce loss to fraud, strengthen customer confidence, comply with government mandates and secure valuable identities and information. It is simple to deploy and does not require direct integration to backend banking applications.

Finalists 2014

- CA Technologies for CA PaymentMinder Risk Analytics
- Entrust for Entrust TransactionGuard
- RSA, the Security Division of EMC, for RSA Silver Tail
- SpectorSoft for Spector 360 Recon
- Trusteer for Trusteer Pinpoint Malware Detection and Trusteer Pinpoint Account Takeover (ATO) Detection

Reader Trust Award

BEST IDENTITY MANAGEMENT SOLUTION

WINNER

NetIQ for NetIQ Identity Manager 4

Identity management has been thrust into the limelight because market conditions and technology shifts toward cloud, mobility and direct customer interaction are dictating just how important identity is to user productivity, security and even business opportunity. Businesses need immediate and easy access to information to react faster to changes in competitive markets. But access must be balanced with controls that secure protected information and address regulatory mandates. NetIQ Identity Manager is architected for real-time, automated response across enterprise, cloud and mobile resources to enable user-friendly access governance, to identify malicious activity by user and support new business initiatives rapidly. It secures the enterprise through identity intelligence that enables secure and user-friendly access to applications. Identity Manager uses integrated identity information to seamlessly create, modify and retire identities, while controlling their access to resources with the synchronization, scalability and high-availability required of large-scale deployments.

Identity Manager is not a one-trick pony, centralizing and automating identity provisioning and access administration from the data center to the cloud. It has redefined enterprise-grade user provisioning by integrating sophisticated roles management, advanced workflow capabilities and intelligence through integration with SIEM tools for identity tracking. Designed to support the identity and compliance needs for the most advanced enterprise or managed service provider, The tool also includes tools for data cleansing, policy framework design and the ability to define roles and entitlements using a simple drag-and-drop functionality, eliminating the need to write code and offering faster time to value.

Reader Trust Award

BEST MANAGED SECURITY SERVICE

WINNER

Sophos for Sophos Complete MSP Security

MSP customers demand affordable, tailored and outsourced IT security that just works. Unfortunately, most security offerings were not built for this reality. Often, MSPs are stuck "making IT work," cobbling together products and adapting services and business models to vendors' constraints. Sophos Complete MSP Security is a partner program that is designed to drive market success for MSPs by aligning with their business and technical needs to bring complete security services to market. Sophos Complete MSP Security also makes offering IT security as a service more profitable. With Sophos' new self-provisioning MSP licensing, this program offers compelling usage-based pricing and pay-as-you-go monthly billing, and requires no up-front commitments.

It is the first MSP-focused solution to offer complete protection for networks, endpoints and mobile devices from a single vendor. MSPs are excited about the Complete MSP Security offering because they no longer have to monitor and manage multiple consoles across client sites and have access to Sophos support.

Complete MSP Security makes offering IT security as a service easier and more profitable. MSPs can offer a full range of IT security services that provide instant credibility and proven protection, including centralized management that allows them to manage all of their customers' locations simply and at no extra charge. The positive feedback from customers, partners and industry experts alike has been overwhelming. "What Sophos is doing with their new MSP program is cutting edge and will be a major game changer for the entire industry," said Shane Swanson, COO, CharTec. "Having the ability to have a true pay-as-you-go offering for our UTM offering is exactly what we as MSPs have been asking for from the industry.

Finalists 2014

- CA Technologies for CA IdentityMinder
- Centrify for Centrify Server Suite Enterprise Edition
- Dell for One Identity Manager
- NetIQ for NetIQ Identity Manager 4
- Ping Identity for PingFederateEnterprise
- RSA, the Security Division of EMC, for RSA Aveksa

SOPHOS

Finalists 2014

- Dell SecureWorks for Dell SecureWorks Managed Security Services
- MANDIANT for MANDIANT Managed Defense
- OpenDNS for Umbrella by OpenDNS
- Sophos for Sophos Complete MSP Security
- Verizon for Managed Security Services

Reader Trust Award

BEST MOBILE SECURITY SOLUTION

WINNER

AirWatch for AirWatch Enterprise Mobility Managment

Mobile devices are proliferating in the enterprise at an exponential rate. With the growing number of device models, platforms and operating system versions available, businesses are facing new and complex mobility management challenges. Accessing corporate resources from a mobile device can introduce a significant threat to corporate security. AirWatch enterprise mobility management (EMM) enables businesses to address challenges associated with mobility by providing a simplified, efficient way to view and manage all enterprise devices from one central console. With AirWatch EMM, organizations can manage a diverse fleet of devices, regardless of platform, device type or ownership. AirWatch's simple enrollment process provides a consistent enrollment flow for all major platforms and allows both administrators and end-users to enroll devices. By simplifying enterprise mobility, AirWatch empowers companies to focus on innovative uses of mobile technology rather than the complexities of managing mobility.

With a fully integrated enterprise mobility management (EMM) suite, including MAM, MDM and MCM, AirWatch offers a robust feature set. Additionally, AirWatch has built a strong network of NAC vendor partnerships, and it has implemented the most OEM-APIs out of any EMM provider.

AirWatch provides an advanced EMM solution at the lowest cost to more than 8,000 of the most scaled, global and security-focused organizations in the world. As a global leader in enterprise-grade mobility solutions, AirWatch has built a scalable solution that grows with its customers, integrates with existing enterprise systems and allows users to manage all devices from one central console.

Finalists 2014

- AirWatch for AirWatch Enterprise Mobility Managment
- Dell SonicWALL for Dell SonicWALL Mobility Solutions (SRA Series)
- F-Secure for F-Secure Mobile Security
- Mobile Active Defense for Mobile Enterprise Compliance and Security Server
- Sophos for Sophos Mobile Control 3.5 (SMC)

Reader Trust Award

BEST MULTIFACTOR SOLUTION

WINNER

Entrust for Entrust IdentityGuard

The Entrust IdentityGuard software authentication platform enables organizations to protect user identities from complex malware and advanced threats while reducing business complexity, risk and cost. Entrust IdentityGuard can be used to authenticate a variety of identities – from privileged-access users to external users applications or even machines and mobile devices. IdentityGuard system administrators or end-users can quickly and easily self-recover or provision entirely new authenticators without deploying new software or modifying backend applications. The Entrust IdentityGuard framework - which manages identities for mobile, cloud and physical/logical access – regularly evolves to empower customers to embrace new identity-based security measures. This helps organizations better manage new threats and more easily embrace technology trends, such as mobile devices or biometrics, as authenticators.

With a breadth of capabilities that span physical and logical access, as well as mobile and cloud, Entrust IdentityGuard empowers customers to effortlessly implement controls and policies to address today's problems on a platform that will grow with them as needs evolve. Entrust IdentityGuard gives customers a working framework that protects identities wherever the identity is being used – for example, gaining physical access at the door to a building, a floor or a restricted area; logging in to the corporate network from a desktop or mobile device; accessing cloud applications with a strong corporate digital identity; integrating with IAM and legacy applications; empowering users with self-servicing applications; protecting mobile devices with a strong digital identity; using mobile devices as strong digital identities; and performing transaction verification on a mobile device via a secure out-of-band channel.

Finalists 2014

- Authentify for Authentify xFA
- CA Technologies for CA Advanced Authentication
- Entrust for Entrust IdentityGuard
- RSA, the Security Division of EMC, for RSA SecurID
- Secure Access Technologies for SAT Mobile ID and Proximity Security
- VASCO Data Security for MYDIGIPASS.COM

Reader Trust Award

BEST NAC SOLUTION

WINNER

Juniper Networks for Junos Pulse Policy Secure

Junos Pulse Policy Secure (formerly Unified Access Control) enables global organizations to secure LAN, cloud, application and data access for all users, regardless of device type and ownership. It enables worldwide government agencies and ministries, financial, health care and other global organizations to ensure a secure, consistent or differentiated network, cloud, application and data access for all users and their devices, while efficiently managing personal mobile device access and BYOD initiatives, limiting access to highly sensitive data to only approved users, ensuring secrecy and security, and maintaining strict adherence to government and industry compliance regulations. Junos Pulse Policy Secure delivers flexible, security-focused, automated access control based on user identity and role, device type and integrity, and location, as well as additional relevant data collected from other disparate network and security appliances and software, leveraging existing infrastructure and software, including deployed mobile device management (MDM) solutions.

Junos Pulse Policy Secure centralizes access and security policy creation, decisions, aggregation and dissemination. Standards-based Junos Pulse Policy Secure insures existing and future network and security investments, working across diverse, heterogeneous network deployments. It works with vendor independent 802.1X-based switches and access points, limiting risk of proprietary lock-in. It simplifies NAC deployment by sharing access and security policies with other network security devices and software, in addition to gathering user, device and session data from those same devices and software, incorporating that info into its policy decision process.

Finalists 2014

- Bradford Networks for Network Sentry
- ForeScout Technologies for ForeScout CounterACT
- Juniper Networks for Unified Access Control (UAC)
- Trustwave for Trustwave NAC

Reader Trust Award

BEST RISK/POLICY MANAGEMENT SOLUTION

WINNER

SolarWinds for SolarWinds Network Configuration Manager

SolarWinds Network Configuration Manager (NCM) effectively enforces enterprise configuration policies for network devices, including firewalls, routers and switches across heterogeneous networks by assessing network device configuration compliance for both internal and industry policies and standards. The product includes out-of-the box support compliance reporting and best practices for Cisco and Juniper devices. Customers can also create their own compliance assessment reports. The solution uses effective change-control workflows allowing proposed configuration changes to be reviewed and approved before being automatically updated. It protects device configurations using automatic backup and easy-to-use restore capabilities, and actively monitors device configurations in real-time for any changes and automatically issue alerts

SolarWinds NCM offers a number of unique capabilities. It is part of the SolarWinds IT management suite and is fully integrated with other powerful IT management tools, including Network Performance Monitor (NPM), Server and Application Monitor (SAM), Network Traffic Analyzer (NTA), IP Address Manager (IPAM), User Device Tracker (UDT), VoIP & Network Quality Manager, Log and Event Monitor (LEM) and more. This suite offers a unified view of the network and a common framework for proactively identifying and resolving network and systems problems. Too, NCM delivers impressive business benefits, including time-to-value and return-on-investment, due to its affordable licensing and maintenance terms and easy-to-use design. Prospects are able to download a fully functioning version, install and be using the product in about 60 minutes.

Finalists 2014

- McAfee for McAfee Real Time for ePolicy Orchestrator
- Rapid7 for Rapid7 ControlsInsight
- RSA, the Security Division of EMC, for RSA Archer
- SolarWinds for SolarWinds Network Configuration Manager
- Tripwire for Tripwire Enterprise Suite

Reader Trust Award

BEST SIEM SOLUTION

WINNER

McAfee for McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) revolutionizes security information and event management (SIEM) by integrating security intelligence with information management for enterprise situational awareness. It connects a real-time understanding of the world outside – threat and reputation data and vulnerability news – with a real-time understanding of the systems, data and activities inside an enterprise.

While McAfee ESM is an appliance-based solution, it offers not only industry benchmarking scale and performance but an ESM solution that is part of the McAfee Security Connected framework, offering active integration into other McAfee security solutions for quickly and intelligently optimizing security posture.

It provides actionable information in minutes instead of hours, and provides massive data collection across a wide range of information sources. It offers real-time threat and risk data integration and event correlation, and immediate access to years of event and flow data, while supporting monitoring and reporting against more than 240 regulations. It also provides integrated tools for improved security workflow, and its flexible, hybrid delivery options include physical and virtual appliances.

Reports and rules are updated weekly or more frequently as volume of updates requires. New releases of the product are typically scheduled several times a year, featuring valuable integrations and enhanced capabilities to support customers' evolving needs in threat and compliance management.

McAfee ESM's ease of deployment and management ensures that customers can meet or exceed their budgeted SIEM project and realize ongoing value in their investment.

In addition, McAfee ESM's compliance reporting delivers timely response to auditor inquiries.

Finalists 2014

- AlienVault for AlienVault Unified Security Management Platform
- HP for HP ArcSight ESM
- LogRhythm for LogRhythm's SIEM and Security Analytics Platform
- McAfee for McAfee Enterprise Security Manager
- SolarWinds for SolarWinds Log & Event Manager
- Splunk for Splunk Enterprise

Reader Trust Award

BEST UTM SECURITY SOLUTION

WINNER

Juniper Networks for SRX Series Services Gateway for the Branch

As the volume and sophistication of attacks accelerate, IT teams are under growing pressure to protect their companies with limited staffing resources and budgets. As such, IT teams require an operationally-efficient solution that meets their broad security needs at an affordable price. SRX for the Branch offers security (including firewall, VPN, UTM content security services) and networking (routing and switching) all in one security gateway. The combination of security services address and mitigate the growing number and types of attacks. In addition, by offering all this functionality in one device, SRX helps IT teams save money and time. The benefits include dealing with one vendor, one management console, less training time, one support team, one reporting and logging tool, etc.

SRX delivers market-proven security with advance routing and switching in a single device. Its partnerships include Websense for enhanced web filtering and two options for anti-virus, and Sophos and Kaspersky for cloud and on-box anti-virus respectively. SRX provides multiple dedicated processing cores and separate data and control planes, assuring higher performance and remote administrative access security.

SRX's high performance throughput and modular architecture enables businesses to maximize their investment. In addition, UTM helps customers address compliance needs and mitigates downtime due to attacks. SRX Series ensures that the network is always available. Whether the gateways are used in pairs for active/active or active/passive high availability or utilizing in-service software updates to ensure network operation while updating the operation system, SRX enables business continuity and employee access.

Finalists 2014

- Barracuda Networks for Barracuda Firewall
- Check Point Software Technologies for Check Point 600 Appliances
- Fortinet for FortiGate-240D
- Juniper Networks for SRX Series Services Gateway for the Branch
- Sophos for Sophos UTM

Reader Trust Award

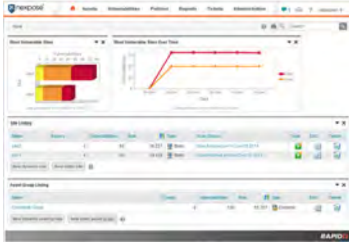
BEST VULNERABILITY MANAGEMENT SOLUTION

WINNER

Rapid7 for Rapid7 Nexpose

Rapid7 Nexpose simplifies security by providing security teams with simple answers to complex security questions. After each security scan of the network, it can generate a one-page report providing recommendations on the top 25 remediation actions that have the biggest positive impact on IT security risks, enabling security teams to focus on the risks that matter. Nexpose proactively scans IT environments for misconfigurations, vulnerabilities and malware while giving guidance for mitigating risks. With Nexpose, security professionals can assess and then act on the security risk within their entire IT environment. This includes networks, operating systems, web applications and databases, giving security teams deep insight into their security threats. Nexpose allows security teams to cover the entire vulnerability management lifecycle, from discovery through remediation. Exploit intelligence, industry metrics and risk scoring are all factored into sequenced remediation roadmaps.

With thousands of vulnerabilities across a system, it can be hard to figure out which ones an admin needs to address first. While a system may have a vulnerability, security controls might be in place that stop attackers from exploiting it. Through its integration with Rapid7 Metasploit, Nexpose can validate vulnerabilities by simulating an attack on the system. If a vulnerability is found to be exploitable, it's equally exploitable by a malicious attacker and should therefore be addressed as soon as possible, making vulnerability validation a pragmatic way to prioritize resources. Many security professionals work with other teams to address vulnerabilities. Nexpose makes it easy to create custom reports tailored to a target audience – for example, including vulnerability reports only for Windows systems if one is sending them to the Windows team.



Finalists 2014

- HP for HP Fortify on Demand
- Qualys for QualysGuard Vulnerability Management
- Rapid7 for Rapid7 Nexpose
- Tenable Network Security for Nessus
- Tripwire for Tripwire IP360

Reader Trust Award

BEST WEB APPLICATION FIREWALL SOLUTION

WINNER

Barracuda Networks for Barracuda Web Application Firewall

A study by Forrester found that 67 percent of vulnerabilities can be found at the application layer. Additionally, as organizations embrace the cloud, a growing concern is how organizations can secure their applications. An Intel study reported that 87 percent of the IT pros surveyed were concerned about security and 28 percent experienced a public, cloud-related breach.

The Barracuda Web Application Firewall blocks an ever-expanding list of application attacks while preventing data loss. It blocks SQL injections, cross-site attacks, DDoS, malware uploads, and more. As new threats emerge, the WAF will automatically gain new capabilities and block them. It inspects outbound traffic to detect sensitive data and either mask or block the traffic. With the new cloud editions of the Barracuda WAF, organizations now have the flexibility to deploy the same strong protection as hardware appliances, virtual appliances or as part of an organization's cloud infrastructure.

Unlike traditional network firewalls or IPS that simply pass HTTP or HTTPS traffic for web applications, the Barracuda Web Application Firewall proxies traffic and inspects it for malicious content. For added security, the Barracuda Web Application Firewall provides full PKI integration for use with client certificates to verify identities of clients accessing the web applications. Barracuda's' approach goes beyond the traditional web application firewall to offer customers load balancing. This provides a unique opportunity for customers to benefit from secure application delivery, reducing impact loads on servers and providing optimal performance and availability. Barracuda has also built a relationship with Microsoft to offer protection for web apps and data hosted in the Windows Azure Cloud.

Finalists 2014

- Barracuda Networks for Barracuda Web Application Firewall
- Dell SonicWALL for Dell SonicWALL SRA 7.0 Web Application Firewall
- Fortinet for FortiWeb-400C
- Juniper Networks for WebApp Secure (formerly Mykonos)
- Trustwave for Trustwave Web Application Firewall

Reader Trust Award

BEST WEB CONTENT MANAGEMENT SOLUTION

WINNER

Websense for Websense Web Security Gateway Anywhere

The content we are accessing on the web is changing, with businesses increasing their use of streaming and social applications and employees accessing this information from mobile or remote locations. Unfortunately, the criminals have tracked this shift and have moved more resources to lures that are mobile, social and visual. This opens the door to malware, data theft, legal liabilities, productivity issues and bandwidth loss. The web is also the portal through which advanced threats enter the network through attacks.

Websense Web Security Gateway Anywhere (WSGA) uses TruHybrid technology to combine on-site appliance and cloud security with a unified console to offer complete protection against malware and data theft for employees in all locations. WSGA also offers TruWeb DLP for data theft and loss protection. Its Advanced Classification Engine (ACE) provides real-time security and data analysis to safeguard organizations from evolving web threats anytime, anywhere.

Websense analyzes and categorizes dynamic web content/threats in real-time, at point-of-click, to detect advanced payloads, exploited documents, mobile malware and much more. Three to five billion requests per day from 900 million endpoints are inspected. It extends hundreds of use policies for social websites that old-school URL filtering cannot accurately classify. Embedded TruWeb DLP enables safe outbound communications, preventing sensitive data disclosure even through scanned images (with OCR), drip DLP and criminally-encrypted control communications.

The tool lowers cost of ownership by consolidating content security capabilities (social media acceptable use policy, network AV, DLP, email security, application controls) through the unified TRITON framework.

websense
websense
WEBSENSE WEB SECURITY GATEWAY ANYWHERE
WEBSENSE WEB SECURITY GATEWAY ANYWHERE
TRITON
TRITON

Finalists 2014

- Blue Coat Systems for ProxySG with WebFilter
- Clearswift for SECURE Web Gateway
- Entensys for UserGate Web Filter
- Trustwave for Trustwave Secure Web Gateway
- Websense for Websense Web Security Gateway Anywhere

Excellence Award

BEST CUSTOMER SERVICE

WINNER

Barracuda Networks for Barracuda Customer Service and Support

Barracuda offers multiple hard copy and online tools to make setup and installation quick and easy for customers. This includes quick-start guides and installation manuals, as well as more detailed administration guides. This documentation outlines step-by-step processes to get up and running quickly and efficiently, as well as tips and best practices to make its products most effective.

The company provides documentation that is easy to understand and is effective. In fact, *SC Magazine* conducted a review of Barracuda's flagship email security offering, published in September 2012: "We found deployment of this product to be quick and easy... We found the quick-start guide to provide an excellent amount of detail on the initial configuration steps to get the appliance up and running in the environment and filtering email with a base configuration."

Barracuda strives to provide fanatical and awesome customer service with live people always on the receiving end to help trouble shoot – there are no phone trees and no automated service.

As well, Barracuda customers are provided with telephone support. Since inception, Barracuda has prided itself on making sure that there is always a live person available to help with any customer issues 24 hours a day, seven days a week. This is included as part of the purchase price at no additional charge.

Barracuda customers also are provided with web-based downloads at no additional charge. This includes a variety of overview information (whitepapers, best practice tips, user guides), as well as set-up quickstarts, admin guides and more.

Further, customers are provided with online forums and FAQ sections online at no additional charge.

Finalists 2014

- Barracuda Networks for Barracuda Customer Service and Support
- DigiCert for DigiCert Customer Service
- IBM for IBM Security
- Qualys for Qualys
- Trustwave for Trustwave

Excellence Award

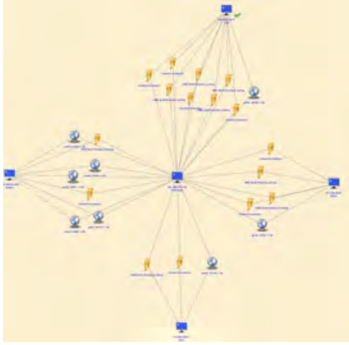
BEST EMERGING TECHNOLOGY

WINNER

21 CT for LYNXeon

As Gartner discusses the futility of perimeter defenses and organizations continue to be frustrated with damaging attacks, the tide is turning toward a more active security approach powered by security analytics and visualization. The challenge to making this shift is how to gain active intelligence quickly, while moving beyond simple search and dashboard intelligence provided by the large security event platforms, so as to arm teams to hunt down the nefarious players hiding in their network. LYNXeon from 21CT is powered by patented graph pattern analytics to collect, fuse and visualize any network data and provide interactive visibility, behavioral analysis and pattern detection that identifies previously missed attackers. Security analysts don't have to wait for an opportunity or threat to arise. Instead they are actively using data already at their disposal to analyze and visualize never-before-seen anomalies, links and relationships.

Each day security analysts need to contend with huge volumes of information as they struggle to fend off attacks. LYNXeon takes over where traditional perimeter security and event management solutions stop. The solution includes a graph database for ultimate analytic performance enabling analysts to conduct faster root cause analysis of events and search for suspicious and malicious traffic patterns over larger sets of historical data. It also includes LYNXeon Connect, an enterprise-grade collection framework that connects with key security data, including network connection data, intrusion detection alerts, malware detection alerts, threat feeds and application metadata. LYNXeon Connect works directly with the LYNXeon Connector Library, which supplies standard data connectors for the industry's leading security products.



Finalists 2014

- 21 CT for LYNXeon
- Carbon Black for Carbon Black
- CloudPassage for CloudPassage Halo
- Juniper Networks for WebApp Secure (formerly Mykonos) featuring Spotlight Secure
- Sourcefire for Sourcefire Advanced Malware Protection (AMP)

Excellence Award

BEST ENTERPRISE SECURITY SOLUTION

WINNER

Splunk for Splunk Enterprise

Splunk has experienced unparalleled growth rates and is one of the fastest growing SIEM vendors in the world, as well as one of the fastest-growing security software vendors overall. For Splunk's last reported quarter ending July 31, 2013, it announced revenue of $66.9 million, which was a growth rate of more than 50 percent from the year before. It also announced 400 new customers for the quarter, taking its total customer count to over 6,000 in over 90 countries.

The company's unique Big Data architecture supports the convergence of security and compliance, operations, application management, web analytics and business intelligence use cases for enterprise operational intelligence, enabling a strong ROI.

Splunk offers worldwide 24/7/365 customer service support via phone or email. It has customer service offices around the globe to ensure, fast, localized support. For customers with support contracts, P1 issues will be responded to immediately. Also, Splunk Education offers a wide range of customer classes that cover installation, administration, advanced searches, and more. For free self-help, Splunk offers a full set of public, easily searchable technical publications covering all major Splunk products. The company also supports a site, called Splunk Answers, where customers, employees and partners answer questions posed by customers. In many cases, answers to questions are turned around in minutes because the site has grown into a vibrant, active community filled with hundreds of users.

The Splunk team is continuously working with customers to gather feedback to better refine the product to meet needs, and to create new features and products they are asking for. At least once a year, the core Splunk Enterprise product undergoes a major release or a significant dot release.

splunk> Enterprise Security
Notable Events by Security Domain
Access
Endpoint
Network
Identity
Audit
Threat
Notable Events by Urgency
Notable Events by Time

Finalists 2014

- FireEye for FireEye Oculus
- ForeScout Technologies for ForeScout CounterACT
- Radware for Attack Mitigation System
- Splunk for Splunk Enterprise
- Tripwire for Tripwire Enterprise Security Suite

Excellence Award

BEST REGULATORY COMPLIANCE SOLUTION

WINNER

Tripwire for Tripwire Enterprise Suite

Tripwire has been providing regulatory compliance to customers for more than 16 years, with more than 2,500 customers that rely on Tripwire Enterprise to prove compliance against everything ranging from PCI, *SOX, NIST, HIPAA*, and more. Reflective of Tripwire's mission as a leading provider of risk-based security and compliance management solutions, its customer base extends into vertical industries including government, energy, financial services, retail, manufacturing, education and entertainment.

Tripwire offers a three-tiered approach to customer services Standard Services offers fundamental assistance to customers just getting started with Tripwire, including local and remote "quick start" packages aimed at rapid implementation. With Custom Services, Tripwire assists customers in streamlining integration of their Tripwire products. Managed Services, also known as Tripwire Remote Operations (TRO), offers customers a trained Tripwire staff member that manages these systems remotely, allowing them to benefit from Tripwire's security and compliance best practices.

Tripwire's training program is designed to provide IT teams with the customizable tools necessary for implementing and managing Tripwire solutions. The training is a combination of both comprehensive coursework and hand-on labs experience, and often culminates in Tripwire certification upon completion of the course exam. It's no wonder the company has 96 percent overall customer satisfaction.

Tripwire Enterprise is updated once a year, adding new features and automation capabilities. Policy and compliance content is updated on a quarterly basis, in cadence with updates to source policies. All of these updates are available from the Tripwire Customer Center to any Tripwire customer enrolled in one of its support programs.

tripwire®

CONFIDENCE: SECURED

Finalists 2014

- Agiliance for Agiliance RiskVision
- AirWatch for AirWatch Enterprise Mobility Managment
- Qualys for QualysGuard Policy Compliance (PC)
- Tripwire for Tripwire Enterprise Suite
- Websense for Websense Data Security Suite

Excellence Award

BEST SECURITY COMPANY

WINNER

Qualys

More than 6,000 customers in more than 100 countries use the QualysGuard Cloud Platform and integrated suite of solutions for a unified view of their security and compliance postures. Customers range from large global organizations to small businesses, served from Qualys' globally-distributed cloud platform delivering powerful IT security and compliance solutions at an affordable cost. With solutions delivered as a service, there is no equipment to install, and subscriptions include free training and support. Qualys can also rapidly deliver new solutions, enhancements and updates to its entire customer base. Over the past five years, revenues and customers have more than doubled and the number of Fortune 1000 customers more than tripled.

Leveraging its cloud platform, Qualys has worked closely with customers over the past 13 years to rapidly and efficiently deliver new solutions, enhancements and security updates, building a comprehensive portfolio of powerful solutions. The QualysGuard Cloud Platform and its integrated suite of security and compliance solutions includes vulnerability management, web application scanning, malware detection service, policy compliance, PCI compliance, Qualys SECURE Seal and web application firewall, enabling customers to automate the lifecycle of asset discovery, security assessments and compliance management across its IT infrastructure and assets, whether they reside inside the organization, on their network perimeter or in the cloud. Since inception, the solutions have been designed to be delivered through the cloud and to be easily and rapidly deployed on a global scale, enabling faster implementation, faster product updates, broader adoption and lower total cost of ownership than traditional on-premise enterprise software products.

Finalists 2014

- AirWatch
- Check Point Software Technologies
- Kaspersky Lab
- Prolexic Technologies
- Qualys
- Trend Micro

Excellence Award

BEST SME SECURITY SOLUTION

WINNER

Barracuda Networks for Barracuda Spam Firewall

The Barracuda Spam Firewall is the world's number-one selling email security appliance. While it is perceived as a replacement market, needs continue to evolve in standard email gateways. The Barracuda Spam Firewall offers fast, easy setup and management. It does not require a dedicated IT expert. The out-of-the-box solution saves resources and lets the IT team focus on other issues. With a wide range of models to choose from, an ideal solution is available regardless of the size of the company, and the integration of the Barracuda Cloud Protection Layer, email encryption and large file transfer with Copy makes it easy to scale capacity as needs change.

Barracuda, has always strived to provide fanatical and awesome customer service with live people always on the receiving end to help troubleshoot – there are no phone trees and no automated service. The experts at Barracuda Central work 24/7 to monitor and block threats.

Competitive pricing with no per user fees makes Barracuda products affordable with no unexpected costs. The Barracuda Spam Firewall is offered in seven models starting at $699 to $89,999, plus flat fees for Energize Updates and Instant Replacement. The Barracuda Instant Replacement program provides a single, convenient subscription that covers users in case of hardware failure and provides an affordable way to migrate to the most current hardware platform on an ongoing basis.

Barracuda Energize Updates provide protection from the latest threats and are sent out hourly or more frequently if needed, to ensure that customers always have the latest and most comprehensive protection. The Barracuda Spam Firewall model 600 recently received a five-star rating from *SC Magazine*, which "found this solution an excellent value for the money."

Finalists 2014

- Barracuda Networks for Barracuda Spam Firewall
- Check Point Software Technologies for Check Point 600 Appliances
- Kaspersky Lab for Kaspersky Endpoint Security for Business
- Qualys for QualysGuard Express
- Sophos for Sophos UTM

Excellence Award

ROOKIE SECURITY COMPANY OF THE YEAR

WINNER

Secure Mentem

For a company that has operated for less than a year, this company has an incredibly impressive customer base, including UPS, The Blackstone Group, Netflix, PayPal, Johnson Controls, among similar organizations. The Blackstone Group is in the process of rolling this provider's offering out to its portfolios companies, which include the likes of Orbitz, Hilton Hotels and Grace Chemicals. Blackstone felt so strongly about the uniqueness and versatility of the company's services that it made an investment in Secure Mentem. Contracts are pending with JPMorgan Chase, Bank of Tokyo, TRW, among others. It also signed a reseller agreement with Accuvant. All of this demonstrates the strength of the current and future customer base.

Secure Mentem provides the entire gamut of security awareness solutions. Its flagship security-awareness-as-a-service solution is unique and patent pending. It provides a turnkey program based on its own study of what organizations actually need. It offers the solutions a la carte as well. Most vendors in the sector provide point solutions, such as collateral materials, computer-based training or phishing. Sometimes, vendors attempt to go into another market sector to increase their revenue potential. However, based on proprietary research, Secure Mentem went into the market intending to provide a comprehensive solution, not disjointed piecemeal solutions that do not support each other.

Secure Mentem was founded on groundbreaking research into the critical success factors of the security awareness programs of Fortune 500 companies. Based on this research, it created its security-awareness-as-a-service program, which provides turnkey security awareness programs that are less expensive and more effective than an organization can create for themselves.

SECURE MENTEM

Finalists 2014

- Appthority
- Gazzang
- Norse
- Prevoty
- Secure Mentem

Professional Award

BEST PROFESSIONAL CERTIFICATION PROGRAM

WINNER

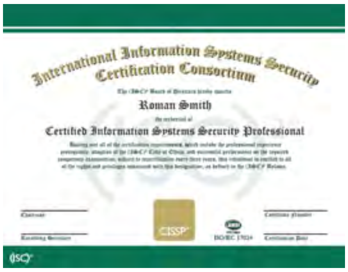
(ISC)² for CISSP

With 90,000+ CISSPs in 137 countries and its recognition as the gold standard of information security credentials, the CISSP is considered the doctorate of certifications for security professionals, according to Crisp360.com. (ISC)2 offers infosec professionals worldwide a variety of education opportunities that enable them to continually refresh and deepen their knowledge and strengthen their connections to the security community. As a globally recognized standard of infosec competence, the CISSP Common Body of Knowledge (CBK) consists of 10 domains, which represent the core infosec concepts professionals need to thrive in the industry today. The CBK is updated quarterly by subject matter experts from the global (ISC)² membership and other luminaries. In addition, the CISSP undergoes a complete analysis annually for relevance to cover emerging technologies. (ISC)² also provides virtual and in-person education opportunities. To assure continuous education, (ISC)² established the Chapter program, now boasting 105 Chapters worldwide serving 10,000 infosec professionals.

Approximately 10,000 candidates fail the rigorous CISSP exam each year. To meet the ever-evolving needs of today's professionals, the CISSP exam undergoes continual assessment, resulting in fresh content every quarter by (ISC)² members and luminaries. The CISSP was an infosec certification of firsts – first to meet ANSI/ISO/IEC Standard 17024 requirements, first to require high-quality, auditable continuing professional education credits, and one of the first to be listed as a job requirement in the DoD 8570.1 Matrix. It is required for most infosec management jobs and recognized by hiring managers, foreign governments, media, and pros worldwide as the benchmark of qualification and professionalism.

Finalists 2014

- GIAC - Global Information Assurance Certification for GIAC Intrusion Analyst (GCIA)
- GIAC - Global Information Assurance Certification for GIAC Security Expert (GSE)
- Guidance Software for EnCase Certified Examiner (EnCE)
- Information System Audit and Control Association for Certified Information Systems Auditor (CISA)
- Information System Audit and Control Association for Certified Information Security Manager (CISM)
- (ISC)² for CISSP



International Information Systems Security Certification Consortium

[illegible]

Roman Smith

[illegible]

Certified Information Systems Security Professional

[illegible]

Chairman

Executive Secretary

CISSP

ISO/IEC 17024

Certificate Number

Certification Date

(ISC)²

Professional Award

BEST PROFESSIONAL TRAINING PROGRAM

WINNER

The SANS Institute for SANS Training

The SANS Institute provides hands-on, intensive immersion training designed to help students master the practical steps necessary for defending systems and networks. Its curricula of over 40 courses encompass cyber defense foundations, intrusion detection, incident handing, forensics, penetration testing, application security, secure coding, management, auditing, and industrial control system security. To help strengthen the knowledge and skills of the infosec community, SANS offers a variety of free resources – from online discussion groups to content-rich blogs. In addition, SANS develops, maintains and makes available at no cost the SANS Reading Room, the industry's largest collection of research documents about various aspects of information security.

SANS differs from most training programs in course content/structure, instructor expertise and delivery options. All SANS authors are practitioners in their fields, thus uniquely qualified to produce relevant, cutting-edge content that reflects current threats and solutions. Course proposals are subjected to a stringent approval process to ensure the highest quality content that is germane to current threats with practical application. SANS faculty, also practitioners, are hand-selected from a steeply competitive pool of applicants, and follow a highly monitored structured path from peer leadership to classroom instructor. The extent to which SANS instructors will engage/work with students to successfully bridge the gap between theory and practice is an advantage often cited by students. Courses are delivered in a variety of ways to support individuals and organizations throughout the world – live training from mentor-led to classroom style, online self-paced or guided with live instruction, and even steamed directly from a live event.

64 Bits for Network +
64 Bits for Interface
2001:0DB8:CCCC:DDDD:EEEE:FFFF:0000:1111
• Host will have multiple IP addresses

Finalists 2014

- Guidance Software for Guidance Software EnCase Training
- InfoSec Institute for Information Security Boot Camps
- (ISC)² for (ISC)² Education Program
- Security University's Holistic Q4 Credential Q/ISP Qualified/Information Security Professional Training Program
- The SANS Institute for SANS Training

Professional Award

BEST SECURITY TEAM

WINNER

Nissan Americas

Under the leadership of CISO Forrest Smith, the Nissan information security team re-launched in 2010 with a focus on developing its core strengths. The team started small and added carefully vetted team members who are skilled at both information security practices and business communications. Rather than "boiling the ocean" by attempting to improve every aspect of its work across the board at one time, the team first set its sights on key services and processes for which they could work toward achieving best-in-class status. Today, within its corporate environment, the information security department is best-in-class.

First and foremost, the Nissan security team deliberately avoids working as a functional "silo." Because the team is skilled in aligning its services and projects with overall business objectives, all members can participate in numerous cross-functional activities and work productively in collaboration with business and project stakeholders. Every individual on Forrest's team works at the top of their performance bracket as set by managers. In addition, Forrest encourages healthy competition within the team so that the performance bar is set very high. Calling themselves a "team of yes," the members are integrated with the business community inside Nissan, communicating with them, taking part in initiatives, and sitting on task forces. In some cases, they have the opportunity to contribute talents and skills that are outside the realm of information security. This gives them the opportunity to know other people and be known as more than staffers executing tasks.

The team has helped the CISO become influential within Nissan and the corporate world through successful, innovative projects that meet business objectives. Each member of the Nissan security team is an expert in his or her area.

Finalists 2014

- Exelis
- Johnson & Johnson Health Care Systems
- Nissan Americas
- Teleperformance Group

Professional Award

CSO OF THE YEAR

WINNER

Forrest Smith, CISO, Nissan Americas

Nissan's core value is innovation and this extends to its approach to IT security. As CISO for Nissan - Americas, Forrest Smith has built a high-performing team of the most skilled security professionals who are the best "fit" for Nissan's IT security culture. He values both strong security/technical skills and business acumen. Because he is committed to fostering relationships between his team members and senior executives, sometimes having his managers present to key executives, he hires security experts who can participate in broader business-oriented security discussions and are not limited to technical details. In keeping with Nissan's core value, Smith has demonstrated a commitment to developing and managing his team in a way that enables them to be creative and innovative in the security solutions they develop. He believes in creating strong mentorship opportunities within the team and training them across various functions in order to support communication and collaboration.

Smith may be one of the few remaining enterprise CISOs who is still highly technical, which enables him to act as a translator and to bridge the technical and business teams within Nissan. He has earned a great deal of credibility within the company and among executives for this capability and believes that being able to communicate at all levels of the organization engenders a great deal of respect. He also believes that having recruited and built a strong team gives him "bench strength." They have earned the right to interact directly with a very high level of executives on a first-name basis and have access to executives. Smith and his team meet on a regular basis with one of the company board members responsible for information security, and have forged a productive working relationship with him and other senior executives.

Finalists 2014

- Jamey Sample, CISO, Pacific Gas & Electric
- Forrest Smith, CISO, Nissan Americas
- Tim Waggoner, chief systems security officer, National Government Services
- Bruce Wignall, CISO, Teleperformance

Professional Award

EDITOR'S CHOICE

© Ofer Maor

WINNER

OWASP

For its ongoing support of the development and maintenance of secure web applications, we are calling out the achievements of the OWASP (Open Web Application Security Project). Its efforts in offering tools and education materials to developers and other security professionals has greatly aided in furthering the advancement of web application security. The nonprofit group does not endorse or recommend commercial products or services. This enables its open network to remain vendor neutral and synergize the collaborative efforts of the leading lights in software security worldwide. It's all about trust, and information security professionals have come to rely on the group's annual Top 10 project – ongoing since 2003 – which delineates the most common flaws present in web apps, thus increasing awareness in the security community of some of the most critical risks facing organizations.

As well, the "Bug Bash," held for three nights in November during the AppSec Conference, is considered one of the biggest application security bug searches in recent time. The event, sponsored by OWASP, gathered security researchers from 30 countries who collaborated to discern security gaps in software that runs the internet and some of the planet's most commonly used applications.

For its advocacy, outreach and teaching, we are delighted to recognize OWASP with this year's Editor's Choice Award.

SC
MAGAZINE

Haymarket Media
114 West 26th Street, 4th Floor
New York, N.Y. 10001
Email: scfeedbackus@haymarketmedia.com
Telephone: 646-638-6008
Fax: 646-638-6150
Web: www.scmagazine.com