MAGAZINE
AWARDS
2013
Honored in the U.S.

Feb. 26, 2013 • San Francisco
Optimistic despite threats

When it comes to data protection and risk management planning, information security professionals are feeling more hopeful than ever. According to our annual “Guarding Against a Data Breach” survey, compared to previous years, a majority of IT security pros say their organizations are taking appropriate steps to protect critical data.

As promising as this feedback is, one has to juxtapose it against the less upbeat happenings of our collective reality. For starters, advanced persistent threats (APTs) and other more methodical and sophisticated cyber crime attacks are becoming the norm, according to most experts. Just look to the recent attacks against The New York Times, Twitter or the U.S. Department of Energy to get a sense of things to come. Internet-based thieves aren’t as easy to catch in the act or stop altogether nowadays, which means organizations have to stop relying on traditional network protections alone and step up their games with advanced monitoring techniques, application and other endpoint controls, better security awareness training and more. Because spear phising, custom malware and targeted attacks are happening at a rate never witnessed before, a data-centric approach to security is now vital, say experts.

And most security pros have to achieve this desired end with flat budgets. I suppose, though, it’s telling that CISOs generally are upbeat despite myriad problems. Improving risk management plans, bettering policies, strengthening training and bolstering controls, along with constantly educating C-level executives about data security being a necessary part of day-to-day activities, are all recurring duties. Yet, survey respondents — SC Magazine readers — are at the ready to tackle these seemingly endless challenges with zeal. And, for a fortunate growing number, undertaking them deftly is paying off as more CEOs and other business leaders register understanding and embrace IT security for what it is — a necessary pillar of good business.

It’s that passion and commitment that drives us every year to celebrate these industry leaders, their many achievements and the varied contributions they make without hesitation to help advance this essential and vibrant industry. Congratulations to you all. — Ilenna Armstrong, VP, editorial, SC Magazine
The Judges

**CO-CHAIR**
Illena Armstrong  
VP, editorial, *SC Magazine*

**CO-CHAIR**
Rich Baich  
CISO, Wells Fargo

Philip Agcaoili  
CISO, Cox Communications

Rebecca Bace  
CEO, Infidel

Jennifer Bayuk  
principal, Jennifer L. Bayuk LLC

Bruce Bonsall  
senior security strategist, BT US&C

Dennis Brixius  
VP and CSO, The McGraw-Hill Cos.

Chris Camacho  
information security officer, The World Bank

Jaime Chanaga  
CEO, The CSO Board

Rafael Diaz  
CISO, Department of Central Management Services, state of Illinois

Rick Doten  
CISO, DMI Enterprise Transformation

Gene Fredriksen  
global CISO, Tyco International

Stephen Fridakis  
senior IT officer, FAO

Pamela Fusco  
director/CISO, Apollo Group

John Johnson  
senior security program manager, John Deere

Cedric Leighton  
colonel, USAF (Ret.); founder and president, Cedric Leighton Associates

Yonesy Nunez  
SVP, Citi

Jim Reavis  
executive director, Cloud Security Alliance

Ariel Silverstone  
CISO, self-employed

Ward Spangenberg  
director, information security, pearl.com

Chenxi Wang  
vice president, Forrester Research

Larry Whiteside  
CISO, Spectrum Health

Spencer Wilcox  
special assistant and lead security strategist, Exelon

Dov Yoran  
CEO, ThreatGRID
SC Magazine would like to thank all of our sponsors for their generous support of the 2013 SC Awards U.S. Their involvement has made this event possible, which helps raise professional standards in the information security industry worldwide.

Bradford Networks
Bradford Networks enables secure network access for corporate-issued and personal mobile devices.

Champlain College
Champlain College has been providing education in the field of digital forensics and cyber security for more than six years.

CipherCloud
CipherCloud provides cloud encryption and tokenization gateways to enable organizations to securely adopt cloud applications.

Entrust
Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries.

ForeScout Technologies
ForeScout enables organizations to accelerate connectivity by allowing users to access network resources without compromising security.

Halon
Halon Security is a prominent technology leader of email security and firewalls, protecting millions of users worldwide.

HP Enterprise Security
HP Enterprise Security provides information security solutions to protect the hybrid enterprise.

IBM
IBM Security offers one of the world’s broadest portfolios of enterprise security products and services.

Imperva
Imperva provides a comprehensive solution for monitoring and controlling all data usage and business transactions across the data center.

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

Schwartz MSL
Schwartz MSL helps technology companies leverage public relations to create visibility and tell their innovative story.

Solutionary
Solutionary reduces the information security and compliance burden, providing flexible managed security and compliance services.

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

Symantec
Symantec is a global leader in security, backup and availability solutions.

West Coast Labs
West Coast Labs is a leader in independent testing, certification and real-time performance validation for information security products.
Welcome from the co-chairman

Reflecting back on information security and cyber threats in 2012 can be quite exhausting. The volume of cyber agitation and threats in the online world is increasing, and the distribution continues to evolve. As an industry, we have been busy, and as a result we have seen many technologies emerge to help address these complex, ever-changing threats to our companies. Innovation and tradecraft are the tools needed to align our security efforts to meet regulatory requirements, ensure compliance, provide actionable cyber threat intelligence and establish proactive techniques to get ahead of the cyber risks. We need to be able to notice indicators of compromise and have good visibility into what is happening within and beyond our own ecosystem. Timeliness of incident identification combined with lapse time taken to address the incident is a key performance indicator of an organization’s ability to address the new reality we live in today. Understanding why an organization is at risk can be even more valuable than the forensics of root cause because the organization may be able to change a behavior, increase operational security or take other actions to deter any possible impact to their business.

Asymmetric practices, innovative solutions, determination to succeed, creativity and dreams can be found tonight in this room. You are all the supply chain to those fighting the cyber threats each day. Your efforts, technologies and ideas enable countless information security professionals to do their jobs. The internet world depends on you, needs you to keep innovating and appreciates your partnership in dealing with the unprecedented threats we all face every day.


Reader Trust Awards

BEST ANTI-MALWARE GATEWAY

WINNER
Symantec for Symantec Web Gateway

Symantec Web Gateway 5.0 is a web security solution that protects organizations against all types of web-borne malware. The tool is powered by Symantec Insight, which provides proactive protection against new, targeted or mutating threats. Insight enhances protection and can’t be evaded or coded around by self-mutating malware. Also, Symantec Web Gateway can integrate with Symantec Data Loss Prevention seamlessly, which allows for a robust web and data loss prevention solution from a single vendor. This helps stop sensitive data from leaving the corporate network via the web, and also allows for users to receive real-time education on company security policies with notifications for policy violations.

Symantec Web Gateway 5.0 presents organizations with many business and technical advantages. Companies can dynamically allocate resources as web traffic increases. SSL encryption capabilities provide safe transmission of web traffic to popular sites that employees and companies often use for business purposes. Real-time scanning of pages as they load prevents any latency in web browsing and decreases calls to the IT helpdesk.

Symantec Web Gateway’s in-depth reporting gives organizations the detailed view they need into their network, to ensure they are protected from today’s complex and dangerous malware related threats.

Symantec Web Gateway’s ability to be deployed as a proxy or cache helps companies save money by reducing bandwidth usage, and avoiding the need to purchase another solution to perform these functions. Customers who already have a valid subscription of Symantec Web Gateway and Protection Suite Enterprise Edition are also entitled to perform a simple upgrade to the new version at no additional cost.

Finalists 2013
- Dell SonicWALL for Dell SonicWALL TZ 215
- McAfee for McAfee Web Protection
- Symantec for Symantec Web Gateway
- Trustwave for Secure Web Gateway
- Websense for Websense TRITON Security Gateway Anywhere
Reader Trust Awards

BEST CLOUD COMPUTING SECURITY

WINNER
Juniper Networks for vGW Virtual Gateway

vGW is a solution specifically designed for virtualization as opposed to a pale retrofitted alternative. Compared to competing solutions, the hypervisor-based vGW delivers protection, throughput, scalability, automated deployment, operational efficiencies and value. vGW has a high-performance stateful firewall, integrated IDS, compliance monitoring/enforcement, VM Introspection, reporting, access controls, AV protection, support for IPv6 and ground-breaking scalability.

vGW offers granular customer resource isolation, layers of protection, superior performance and regulatory compliance mechanisms that help users trust in the security of their data – and online business. vGW can help organizations take advantage of cloud computing sooner rather than later, optimize investments in virtualization infrastructure and make the most of existing network security investments. It accomplishes this by providing cloud-enabling, purpose-built security and integrating virtualization security with physical network security.

Organizations want to virtualize to save money. Yet, many still hesitate to virtualize because of security concerns. vGW removes barriers to virtualizing, as well as to implementing large-scale virtualized environments for global organizations and cloud service providers. How? By ensuring security doesn’t impede virtualized workload performance and, moreover, maximizing secured VM-to-host compression ratios. With vGW, businesses can plan to support more VMs on a host while ensuring security and without compromising performance.

vGW was built specifically for virtualized environments and takes a fast-path approach to security. Thanks to this design, vGW can clearly and positively impact budget.

Reader Trust Awards

BEST COMPUTER FORENSIC TOOL

WINNER
Guidance Software for EnCase

Guidance Software’s EnCase software is a powerful solution that provides the foundation for government and law enforcement agencies 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. EnCase allows customers to conduct more complete investigations than its competitors with additional integration to CaseCentral’s secure hosted review platform and with security information and event managers (SIEM) for automated incident response. EnCase software includes the EnCase Enterprise platform with software applications EnCase Cyber Security and EnCase eDiscovery built on top of the platform. The product line also includes EnCase Forensic and EnCase Portable.

The tool provides security specialists, investigators, computer incident-response teams and litigation specialists with everything they need 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 for virtually any business purpose. Moreover, users of the EnCase solution have the ability to customize how the solution functions, adding capabilities to the product to meet their specific needs.

With EnCase, organizations can improve effectiveness of their staff, as processes and procedures associated with the acquisition, analysis and reporting of a forensic investigation can be automated, eliminating redundant manual work. This allows examiners to focus on their specialty of completing digital investigations.

Finalists 2013

- IBM for IBM Cloud Security Services
- Juniper Networks for vGW Virtual Gateway
- Sophos for Sophos SafeGuard 6
- Symantec for Symantec O3 Cloud Identity and Access Control
- Websense for Websense TRITON Enterprise

Finalists 2013

- AccessData Group for Forensic Toolkit (FTK)
- FireEye for FireEye Malware Analysis System
- Guidance Software for EnCase
- RSA, the security division of EMC, for RSA NetWitness
- Websense for Websense Cyber Security Intelligence (CSI) On-Demand
Reader Trust Awards

BEST DATA LEAKAGE PREVENTION (DLP)

WINNER
Symantec for Symantec Data Loss Prevention

Symantec Data Loss Prevention delivers a unified solution to discover, monitor and protect confidential data wherever it is stored or used. Symantec offers comprehensive coverage of confidential data across endpoint, network and storage systems – whether users are on or off the corporate network. By measurably reducing risk, Symantec gives organizations confidence to demonstrate compliance while protecting their customers, brand and intellectual property (IP).

Symantec Data Loss Prevention v11.6 is the current release of Symantec’s data security suite. It introduces expanded data loss coverage, advanced multidimensional reporting, improved usability and new security integrations. It features DLP for Mobile, which monitors and protects sensitive data sent from an iPad and iPhone mail client, browser and apps, like Facebook, Twitter and Dropbox. It also secures sensitive data without stopping business or personal use.

Protecting IP is a significant challenge for organizations because it is spread out, and subtle differences between what is sensitive and what is not make finding it time-consuming and costly. With ever-increasing amounts of sensitive data in corporate environments and accessed on mobile devices, with or without permission from IT security, traditional DLP detection technologies cannot effectively and accurately identify and protect IP, like source code documents that change daily. Collecting and fingerprinting 100 percent of confidential data is too time-consuming and expensive, while identifying the data with keywords sacrifices accuracy. Symantec DLP 11 enables organizations to easily define and locate their unstructured data so that they can quickly prioritize which data needs to be fixed, saving time and money.

Reader Trust Awards

BEST DATABASE SECURITY SOLUTION

WINNER
McAfee, an Intel company, for McAfee Database Security Solution

Databases store information, the crown jewels of today’s organizations. For this reason, they are targeted in the overwhelming majority of breach attempts by external hackers and malicious insiders. Perimeter security and the security features of native database management systems (DBMS) prove insufficient as the critical last line of defense for the sensitive, valuable information that databases hold. McAfee Database Security offers real-time, reliable protection for business-critical databases against external, internal and even intra-database threats.

This non-intrusive, software-only solution requires no architectural changes, database downtime or additional security management silos. With this tool, organizations of all sizes can gain complete visibility into their overall database landscape and security posture, fully align their security policy administration practices and efficiently maintain regulatory compliance.

By delivering a complete family of products, fully integrated through McAfee ePolicy Orchestrator’s dashboard, McAfee significantly simplifies the deployment and monitoring of the security infrastructure. McAfee Database Activity Monitoring requires no changes to the database itself and no configuration changes to the network, and yet can provide real-time alerting or session termination with minimal overhead. The memory-based sensor model catches threats from all potential sources, including privileged users, and the fully distributed architecture also can be deployed in virtualized environments and in the cloud. McAfee Virtual Patching for Databases identifies and blocks attempts to exploit known vulnerabilities on unpatched servers, as well as common threat vectors of many zero-day attacks.

Finalists 2013

• Dell SonicWALL for Dell SonicWALL E-Class Network Security Appliance (NSA) 8510
• Identity Finder for Identity Finder
• RSA, the security division of EMC, for RSA DLP
• Symantec for Symantec Data Loss Prevention
• Trend Micro for Trend Micro Integrated Data Loss Prevention
• Websense for Websense Data Security Suite

Finalists 2013

• BeyondTrust for PowerBroker Database - Monitor & Audit
• DB Networks for Adaptive Database Firewall ADF-4200
• IBM for IBM InfoSphere Guardium
• Imperva for Imperva SecureSphere
• McAfee, an Intel company, for McAfee Database Security Solution
Reader Trust Awards
BEST EMAIL SECURITY SOLUTION

WINNER
Barracuda Networks for Barracuda Email Security

Productivity losses due to spam and other email security issues can cost businesses millions of dollars each year. The Barracuda Email Security solutions, including the Barracuda Spam & Virus Firewall appliance and the Barracuda Email Security Service cloud solution are extremely powerful and provide complete email protection for organizations of all sizes.

The email security solution features ease of use and deployment for hardware, virtual, cloud and hybrid offerings with no per-user fees. It provides detailed email monitoring; scans outbound emails and attachments; and blocks disclosure of sensitive data, such as Social Security and credit card numbers. Its outbound scanning also blocks spam from leaving an email server causing reputation loss and blacklisting. Too, the integrated cloud encryption service lets users encrypt customized emails – at no extra cost.

Barracuda Networks leverages 12 defense layers to provide defense capabilities for any email server within large corporate or small business environments. Online resources are available and include a portal for opening a support case, a searchable knowledge base, technical support forum and more.

Without software to install or modifications required to existing email systems, installation of the Barracuda email security solutions are quick and painless.

As well, a key technical advantage for enterprises or SMEs deploying a Barracuda email security solution is access to Barracuda Central, an operations center that works 24/7 to capture the latest data on spam and other email threats from a vast network of honeypots, as well as submissions from the more than 85,000 Barracuda Networks customers worldwide.

Reader Trust Awards
BEST ENTERPRISE FIREWALL

WINNER
Check Point Software Technologies for Check Point R75.40

Internet use has changed dramatically with the wide adoption of virtualization, mobile computing and Web 2.0 in the enterprise. Security used to be handled by simply blocking specific applications, ports or websites entirely. However, the Web 2.0 also drives communication through fewer ports and protocols.

Check Point R75.40 includes Check Point ThreatCloud, the first collaborative network to fight cyber crime. It gathers data from global threat sensors and distributes threat intelligence to security gateways around the globe. The tool also features new anti-bot and enhanced anti-virus software blades, powered by ThreatCloud. Check Point GAia adds a unified secure operating system for all Check Point appliances, open servers and virtual systems. SmartLog is a new feature of the logging and status software blade that provides split-second search results from billions of log records.

Check Point R75.40 allows companies to consolidate security protections with an integrated solution that can be tailored to meet specific security and performance needs. Because R75.40 is based on Check Point’s Software Blade Architecture, customers can expand their security as needed without new management or hardware. This significantly reduces costs.

The tool’s newest security appliances are designed to optimize all of the software blade protections available with R75.40 and leverage the company’s multi-core and acceleration technologies – delivering outstanding firewall performance capable of up to 200 Gbps throughput and less than five-microsecond latency. The result is an integrated firewall solution that keeps businesses safe and information available, without impacting network performance.

Finalists 2013

• Barracuda Networks for Barracuda Email Security
• McAfee for McAfee Email Protection
• Proofpoint for Proofpoint Enterprise Protection/Proofpoint Enterprise Privacy
• Symantec for Symantec Messaging Gateway
• Websense for Websense Email Security Gateway Anywhere

Finalists 2013

• AT&T for AT&T Network-Based Firewall Service
• Check Point Software Technologies for Check Point R75.40
• Dell SonicWALL for Dell SonicWALL SuperMassive E10800
• Fortinet for FortiGate-800C
• Sourcefire for Sourcefire Next-Generation Firewall (NGFW)
BEST FRAUD PREVENTION

WINNER
RSA, the security division of EMC, for RSA Adaptive Authentication

As organizations migrate customers and partners to the web, they must look at two primary considerations: Implementing flexible security that adapts to the ever-evolving world of online threats, and doing so without sacrificing usability.

RSA Adaptive Authentication is a comprehensive, risk-based authentication and fraud detection platform that balances security, usability and cost. Powered by the RSA risk engine, Adaptive Authentication monitors and authenticates online activities in real-time by correlating behavioral analysis, device profiling and data feeds from RSA eFraudNetwork. Because the Risk Engine works behind the scenes to validate devices and behavior, the vast majority of users are authenticated invisibly, without impact to their user experience. Available in both SaaS and on-premise deployments, it is scalable to millions of users, and provides login and transaction protection for users accessing websites, mobile applications/portals, SSL VPN applications and web access management applications.

As a risk and policy-based platform with the ability to leverage the depth of the eFraudNetwork, RSA Adaptive Authentication helps organizations drastically improve fraud detection in real-time, thus decreasing fraud-related losses. In addition, its flexibility lowers operational overhead associated with deployment (i.e., there are no tokens to deploy and users can self-enroll). Most end-users are authenticated invisibly, causing the end-user little disruption, allowing them to access data faster and more efficiently. Finally, offering a solution that does not require tokens or extra passwords means fewer “lost token” or “forgotten password” calls to tech support.

BEST IDENTITY MANAGEMENT APPLICATION

WINNER
CA Technologies for CA IdentityMinder

Managing the identities and access of users to key resources is a critical function for IT organizations under increasing pressure to cut operating costs while demonstrating continuous compliance. They must also deal with other challenges like protecting critical systems, applications and information from unauthorized access and use; increasing efficiency and productivity, without sacrificing security across many platforms; efficiently prove proving compliance with internal policies, regulations and best practices; and easily adopting new technologies – such as virtualization and cloud – that support business initiatives.

CA IdentityMinder helps improve the operational efficiency and effectiveness of IT organizations by providing a scalable and configurable identity management foundation that can organize identity information across the enterprise and within the context of business roles and processes. It helps streamline the on- and off-boarding of users, enables the business to manage access requests and automates identity compliance processes from distributed and mainframe environments.

The tool provides a highly scalable end-to-end solution for automating and improving the many time-consuming tasks associated with identity management. The CA solutions for identity management also build structure around the complete identity lifecycle, enabling repeatability and the ability to leverage standardized processes for additional improvement.

CA IdentityMinder delivers a scalable and configurable solution that accommodates enterprises’ unique needs at every level – from leveraging a role foundation that accurately represents their organizational structure to defining and enforcing unique business and regulatory policies to cost effectively extend automated provisioning to applications and policies.

Finalists 2013
- CA Technologies for CA RiskMinder
- Entrust for Entrust TransactionGuard
- RSA, the security division of EMC, for RSA Adaptive Authentication
- Symantec for Symantec Code Signing
- Trusteer for Trusteer Pinpoint

Finalists 2013
- CA Technologies for CA IdentityMinder
- Centrify for Centrify Suite 2012
- Cyber-Ark Software for Privileged Identity Management Suite
- IBM Security Systems for IBM Security Identity Manager
- NetIQ for NetIQ Identity Manager 4
Reader Trust Awards

**BEST INTRUSION DETECTION/PREVENTION PRODUCT**

**WINNER**

Check Point Software Technologies for Check Point IPS Software Blade

Today’s threat landscape is dynamic, evolving and includes organized groups creating sophisticated attacks that specifically target the security weaknesses of their business target. Enterprises want to protect their business against the multitude of threats while simplifying their security deployment and reducing their total security costs.

The Check Point IPS Software Blade provides complete, integrated, next-generation firewall intrusion prevention capabilities at multi-gigabit speeds, resulting in IPS security and performance. The tool provides complete threat coverage for clients, servers, OS and other vulnerabilities, malware/worm infections and more. The Multi-Tier Threat Detection Engine combines signatures, protocol validation, anomaly detection, behavioral analysis and other methods, including identity and application awareness, to provide the highest levels of network IPS protection. By quickly filtering 90 percent of incoming traffic without requiring deep inspection, the IPS engine inspects for attacks only on relevant sections of the traffic, thus reducing overhead and increasing accuracy.

Customers require the flexibility of the Software Blade Architecture to enable more security functions as needed, ultimately migrating toward a next-generation firewall type of deployment. The IPS Software Blade leverages a sophisticated engine that uses multiple methods of detection and analysis to detect bad traffic and IPS Update Service delivers leading IPS coverage including our industry leading coverage of Microsoft applications.

Deploying the IPS Software Blade dramatically reduces the complexity of customer network security infrastructure by reducing their hardware footprint, rack space, cabling, cooling, as well as power consumption.

**Finalists 2013**

- Check Point Software Technologies for Check Point IPS Software Blade
- Dell SonicWALL for Dell SonicWALL SuperMassive E10200
- HP Enterprise Security for HP TippingPoint
- IBM for IBM Security Network IPS / Network Protection
- Sourcefire for Sourcefire Next-Generation IPS (NGIPS)

Reader Trust Awards

**BEST IPsec/SSL VPN**

**WINNER**

Juniper Networks for MAG Series Junos Pulse Gateways

The Juniper Networks MAG Series Junos Pulse Gateways are a market-leading SSL VPN platform that provide secure remote access for both non-mobile and mobile devices. The offering secures clientless access to enterprise applications, data and resources, and ensure best-in-class endpoint security, granular access control and threat prevention. The MAG Series are scalable for companies of all sizes and support BYOD initiatives through support of all major mobile OSs. In addition to secure connectivity via SSL VPN, MAG Series gateways also can deliver NAC and application acceleration, offering a significant reduction in OpEx and CapEx costs, increased deployment density, extensive scalability and easily reconfigurable “personality” changes between secure mobile and remote SSL VPN access control and network access control (NAC) modes. Juniper’s SSL VPN capabilities are also available as a virtual appliance, offering added flexibility and scalability and lower cost.

The MAG Series Junos Pulse Gateways product family includes models sized to meet the needs of SMBs with limited IT experience, all the way up to high capacity products for large enterprises and service providers requiring the utmost authentication, authorization and accounting capabilities for employee, partner (extranet) and customer access. In addition, a virtual SSL VPN appliance is available.

The solution uses SSL, with no client software deployment required, and offers cross-platform support across any web-enabled device and all major OSs, including Windows, Mac, Linux, iOS, Android and others. Additionally, Host Checker scans endpoints for compliance, including mobile devices used in BYOD, and the tool enables single sign-on capabilities to clouds and web-based applications via SAML 2.0.

**Finalists 2013**

- Barracuda Networks for Barracuda SSL VPN
- Dell SonicWALL for Dell SonicWALL Aventail E-Class SRA EX9000
- HOB GmbH & Co. KG for HOB RD VPN
- Juniper Networks for MAG Series Junos Pulse Gateways
- NCP Engineering for NCP Secure Enterprise Management 3.0
WINNER
Verizon Business for Managed Security Services - Commercial

The continued increase of new technologies and systems introduced to the workplace results in an ever-wider spectrum of business risks – in addition to the challenge of maintaining appropriate technical risk levels, which present themselves as operational challenges, vulnerabilities and evolving internet threats. In order to reduce risk, organizations must move away from standalone and isolated security products as they only provide an incomplete view of enterprise security.

In order to reduce risk exposure, businesses need a methodology and a security platform to manage risk exposure which allows them to anticipate problems, take corrective action and demonstrate results. Verizon offers a process framework and global infrastructure for consistency in handling threats and policies, as well as direct access to experts and best practices. As a result, organizations have one consistent view of their security and risk management posture.

Customers leverage Verizon’s expertise and global infrastructure to address a wide range of challenges, including cyber threats, regulatory compliance and the adoption of cloud-based computing services. The SEAM engine is Verizon’s intellectual property and provides the technology to detect security incidents and to assign a risk rating, which allows the customer to define the business impact based on their asset information. Security incident creation is based on threat information generated by the security devices. Verizon can help determine risk and its impact by taking into account threat, vulnerability, and assets through its proprietary SEAM engine, and can provide valuable insight on recommending corrective action when mitigating threats.

Finalists 2013
• Dell SecureWorks for Dell SecureWorks Managed Security Services
• IBM for IBM Managed Security Services
• Mandiant for MCIPT Managed Defense
• Verisign for Verisign MalDetector Service
• Verizon Business for Managed Security Services – Commercial

WINNER
Marble Security (formerly IronKey) for Marble Access

Criminals, hackers, hacktivists and hostile governments are attacking mobile devices and desktops to steal information, break into online accounts and humiliate governments and enterprises. Marble Security’s Marble Access provides an impenetrable layer of mobile, desktop and network security that protects all endpoints from all threats, both known and unknown, including keystroke loggers, viruses, man-in-the-browser trojans, zero-day malware, malicious Wi-Fi hotspots, network hackers and poisoned DNS attacks. Marble Access provides a unified user experience across PC, Mac, Android and iOS mobile devices. Marble Access combines a virtualized secure browser with encryption, mutual authentication, URL whitelisting and Marble Access technology to isolate users from any threats on the device or the internet.

Personal data is never stored on the device, and cannot be stolen or leaked. At the same time, Marble Access reduces IT costs, secures broader use of the cloud, achieves compliance and risk management goals and enables secure use of BYOD initiatives.

Marble Access differs starting with its virtualized secure browser. Unlike signature-based countermeasures, such as anti-virus or firewalls that are vulnerable to zero-day attacks, the secure browser works with jailbreak detection, keyboard encryption and other technologies to isolate users inside an invulnerable “cocoon.” Marble Access delivers a unified user experience on all platforms: iPhones, iPads, Android, BlackBerries, PCs or Macs. Another major differentiator, the Marble Access, uses encryption, authentication, whitelists, blacklists and other technologies to protect against phishing and network-level attacks, such as DNS poisoning or malicious hotspots.
WINNER

RSA, the security division of EMC, for RSA SecurID

Protecting access to information – and assuring the identities of users requesting that access – is a core element of any security initiative. Whether a small organization or large enterprise, password authentication is not enough to protect against today's security landscape. An additional layer of protection is required.

RSA SecurID is the standard for two-factor authentication solutions. It reliably proves the identities of users, devices and applications by using a unique symmetric key combined with a proven algorithm to generate a one-time password that changes every 60 seconds. RSA SecurID helps legitimate users gain secure access to VPNs, wireless access points, applications in the cloud, on the web and mobile, and network operating systems. Adding in that additional layer, RSA SecurID helps organizations protect private information and assure the identities of people, devices and applications exchanging that information.

RSA offers a broad range of easy-to-use form factors to suit a variety of organizations and requirements. These include both hardware and software authenticators to support the leading mobile platforms, SMS authenticators and software developer kits to custom build API calls into third-party mobile applications.

RSA has more than 400 partners to ensure out-of-the-box integrations with the widest range of applications that are jointly tested by each organization to ensure a positive experience that significantly reduces deployment, testing and integration costs.

RSA SecurID is a cost-effective way for organizations to address authentication and compliance concerns and provide an extra level of security for networks, VPNs, and other business assets. RSA SecurID offers a broad array of form factors and authentication mechanism to meet all budgets.

Finalists 2013

• CA Technologies for CA AuthMinder
• Entrust for Entrust IdentityGuard
• PhoneFactor, a Microsoft company, for PhoneFactor
• RSA, the security division of EMC, for RSA SecurID
• Symantec for Symantec VIP

Reader Trust Awards

BEST MULTIFACTOR PRODUCT

WINNER

RSA, the security division of EMC, for RSA SecurID

Best MultiFactor Product

Finalists 2013

• CA Technologies for CA AuthMinder
• Entrust for Entrust IdentityGuard
• PhoneFactor, a Microsoft company, for PhoneFactor
• RSA, the security division of EMC, for RSA SecurID
• Symantec for Symantec VIP

Reader Trust Awards

BEST NAC PRODUCT

WINNER

Trustwave for Trustwave NAC

Trustwave offers full network access control protection for all endpoints, managed and unmanaged, and works in any network infrastructure. Trustwave NAC combines agentless network access control with zero-day threat prevention and automated policy enforcement and is available in three configurations:

Enterprise NAC – A highly scalable, full-cycle NAC solution designed for large organizations with thousands of endpoints, providing centralized and unified web-based management with unified configuration and reporting support, deployed virtually inline.

Managed NAC – Trustwave's MSS operation offers full-function NAC as a managed service, including the same feature/function support as Enterprise NAC, while maintaining sensor integrity and health, and providing reduced cost with no capital expense.

Plug-n-Play NAC – Offered as an add-on software module with Trustwave’s Managed UTM service for smaller, distributed enterprises, Plug-n-Play NAC automatically detects and optionally blocks rogue devices and network service, providing automatic updates of firewall rules for access policy enforcement.

Agentless deployment works for every endpoint regardless of device type or operating system, including BYOD assets, enabling an organization to quickly start monitoring both existing and new devices that come on and off the network.

The solution requires zero integration with existing switch fabrics or a lengthy implementation process for discovery or enforcement. Trustwave NAC operates virtually inline as needed with a fail-open architecture and self-contained enforcement, with zero latency.

Any device on the network is detected, and patented technology further identifies rogue devices as well as unauthorized routers and gateways.

Finalists 2013

• Bradford Networks for Network Sentry
• ForeScout Technologies for ForeScout CounterACT
• StillSecure for StillSecure Safe Access
• Trustwave for Trustwave NAC
Reader Trust Awards

BEST POLICY MANAGEMENT SOLUTION

WINNER
SolarWinds for SolarWinds Network Configuration Manager (NCM)

SolarWinds Network Configuration Manager (NCM) simplifies managing network configuration files in multi-vendor network environments by backing up configuration files, as well as continuously monitoring device configurations and providing immediate notification of configuration changes to help resolve problems before they impact users.

SolarWinds NCM can check regulatory compliance of all network devices, including routers, switches and firewalls, and generate detailed reports from a single instance. These reports can be launched on-demand or scheduled on a periodic basis and emailed to security personnel.

The compliance checks available cover many different standards, including HIPAA, SOX, PCI, DISA STIG and FISMA, and can be customized by the users based on their company-specific rules and best practices. Users also can create their own checks from scratch. Both customized and entirely new checks can be shared on thwack, the SolarWinds online IT management community.

NCM combines powerful network configuration management features, rapid time-to-value, an easy-to-use web-based interface, and affordability into one package. NCM is part of SolarWinds’ IT management suite, which includes solutions for network, application and server, log and security information, virtualization, storage, IT help desk, remote support and mobile IT management, and real-time troubleshooting and diagnostic tools.

Additionally, SolarWinds’ unique thwack.com community of more than 100,000 members is extremely active. In particular, the NCM section, one of the most active areas of thwack, receives on average dozens of postings per day – questions and answers, shared content, blog postings, feature requests and tips.

Reader Trust Awards

BEST SECURITY INFORMATION/EVENT MANAGEMENT (SIEM) APPLIANCE

WINNER
Splunk for Splunk Enterprise

Splunk is a Big Data security intelligence platform that is used by more than 1,500 customers to search and investigate, proactively monitor user and machine behavior, perform statistical analysis to identify anomalies and unknown threats, and create dashboards and visualizations for executives.

Splunk’s architecture makes all machine data in an organization usable and valuable to the IT security team. It can index any type of machine or log data without upfront normalization, and allows users to create correlations and reports on the raw data. The platform is agile, flexible and lets security customers address a wide range of security use cases – from basic log management and incident investigation/forensics to fraud detection and correlation/alerting – to find known and unknown threats.

In regards to traditional SIEM use cases, the Splunk App for Enterprise Security comes with out-of-the-box reports, dashboards, incident workflow and correlation searches for SIEM use cases.

Splunk can ingest any type of machine data from any source, whether from files, syslog, a script, and more. Splunk stores this data in a flat file data store, not a fixed-schema SQL database, so is not limited to indexing and searching only data that fits a database schema.

Splunk leverages a powerful search technology and language that enables fast, advanced searches against terabytes of data to find threats. Searches can leverage Boolean and statistical logic to identify outliers and abnormal behavior that may represent an advanced, unknown threat. Also, Splunk is software-only and installs on commodity hardware, thus is cheaper and easier to upgrade.

Lastly, Splunk enables the fast creation of new reports and dashboards.

Finalists 2013

- IBM for IBM Endpoint Manager
- AirWatch for AirWatch Enterprise Mobile Management
- NetIQ for NetIQ Secure Configuration Manager
- SolarWinds for SolarWinds Network Configuration Manager (NCM)
- Tripwire for Tripwire Enterprise 8.2

Finalists 2013

- HP Enterprise Security for HP ArcSight
- IBM for IBM Security Q Radar SIEM
- LogRhythm for LogRhythm
- NetIQ for NetIQ Sentinel 7
- SolarWinds for SolarWinds Log & Event Manager (LEM)
- Splunk for Splunk Enterprise
Reader Trust Awards
BEST UTM SECURITY

WINNER
Symantec for Symantec Endpoint Protection

Last year, attackers unleashed more than nine new mutated viruses every second of every day, resulting in more than 403 million distinct threats. This huge volume and variety of threats has made it virtually impossible for security companies to protect users. Traditional security software is reactive, looking for digital fingerprints of viruses after they have been discovered. But today’s criminals work differently, mutating their malware and creating new, unique threats for each user.

Symantec Endpoint Protection v12 offers advanced protection while improving system performance to businesses of all sizes. It includes a new detection system that includes Symantec Insight, a cloud-based technology that tracks more than three billion files from more than 200 million systems to identify new and rapidly mutating threats, as well as SONAR, Symantec’s system for real-time monitoring and blocking of malware. Symantec Endpoint Protection protects both physical and virtual systems.

By tracking nearly every program file on the internet, Symantec can identify new or rapidly mutating files. Leveraging, Insight and SONAR technologies, Symantec Endpoint Protection blocks new and unknown threats missed by traditional signature, heuristic, behavioral and HIPS-based security solutions.

Symantec Insight provides performance advantages. Because Insight knows the security status of most of the files on a system before it scans them, it eliminates up to 70 percent of scan overhead – providing performance so fast users won’t know it is there.

Symantec Endpoint Protection 12 provides unrivaled security, blazing performance and optimization for virtual environments. The tool offers comprehensive defense against all attacks on physical and virtual systems.

Finalists 2013
- Check Point Software Technologies for Check Point 2200 and 4000 Series Appliances
- Dell SonicWALL for Dell SonicWALL TZ 215
- Fortinet for FortiGate-100D
- Sophos for Sophos UTM 9
- Symantec for Symantec Endpoint Protection 12

Reader Trust Awards
BEST VULNERABILITY MANAGEMENT TOOL

WINNER
Qualys for QualysGuard Vulnerability Management

QualysGuard Vulnerability Management (VM) automates network auditing and vulnerability management across organizations, including network discovery and mapping, asset management, vulnerability reporting and remediation tracking. Driven by a comprehensive knowledge base of known vulnerabilities, it enables cost-effective protection against vulnerabilities without substantial resource deployment. It is used by more than 5,800 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100.

Delivered as a cloud solution accessible from any web browser, QualysGuard VM is easy to deploy and manage – even across globally distributed environments – enabling organizations to accurately scan their networks and applications to identify and fix vulnerabilities and collect compliance data. Organizations report 50 to 90 percent lower costs and can more efficiently remediate vulnerabilities using the solution’s powerful tools and features, including centralized reports, verified remedies and risk rankings to prioritize remediation steps, and full remediation workflow capabilities with trouble tickets.

QualysGuard VM delivers a powerful, scalable solution at a low cost. It requires no infrastructure to deploy or manage, saving time and resources, providing a continuous view of security across the organization.

Qualys also maintains the industry’s largest vulnerability database, updated daily for more than 35,000 unique vulnerabilities. Automated signature regression testing ensures quality/accuracy, scoring six sigma accuracy (fewer than 3.4 defects per million scanned). Updates are rolled out immediately, and users can scan globally without requiring additional infrastructure.

Finalists 2013
- GFI Software for GFI LanGuard 2012
- Qualys for QualysGuard Vulnerability Management
- Rapid7 for Rapid7 Nexpose
- Tenable Network Security for Tenable Security Center
- Trustwave for TrustKeeper Vulnerability Manager
Reader Trust Awards
BEST WEB APPLICATION FIREWALL

WINNER
Barracuda Networks for Barracuda Web Application Firewall

A recent study by Forrester Research found that 67 percent of vulnerabilities can be found at the web application layer. The Barracuda Web Application Firewall is a complete and powerful security solution for web applications and websites. The tool quickly protects web servers from data breaches, and websites from defacement, without administrators waiting for clean code or even knowing how an application works.

Additionally, it can increase the performance and scalability of these applications. Content caching, data compression and SSL acceleration optimize application performance while reducing impact on servers. Integrated load balancing further optimizes performance and provides high availability.

Unlike traditional network firewalls or intrusion detection systems that simply pass HTTP or HTTPS traffic for web applications, the Barracuda Web Application Firewall proxies traffic and inspects it for access by hackers. For added security, the solution provides full PKI integration for use with client certificates to verify identities of clients accessing the web applications.

The Barracuda Web Application Firewall performs deep inspection of all web traffic, enabling it to provide a wide range of intrusion prevention capabilities at both the network and application layers. It provides protection from common attacks on web applications, including SQL injections, cross-site scripting attacks, session tampering and buffer overflows. As a full proxy, the Barracuda Web Application Firewall blocks or cloaks attacks, while preventing sensitive outbound data leaks of information.

Overall, customers benefit significantly from ensuring data, applications and websites are secure – and that bandwidth and performance are optimized.

Reader Trust Awards
BEST WEB CONTENT MANAGEMENT PRODUCT

WINNER
Websense for Websense Web Security Gateway Anywhere

Web access opens the door to malware, data theft, legal liabilities, productivity issues and bandwidth loss. In early 2012, 42 percent of Facebook activity was streaming media, many with video lures to malware. Also, there’s been an increase in spear phishing with embedded links to advanced threats. Too, Osterman Research says the costs associated with a malware infection are approximately $110 per user.

Clearly, new technology is needed to reduce these costs. Websense Web Security Gateway Anywhere meets that need with zero-day malware prevention and DLP to address risks not covered by basic URL filtering, anti-virus and firewall solutions.

Websense Web Security Gateway Anywhere (WSGA) offers complete protection against malware and data theft. It uses TruHybrid technology to combine on-site appliances with cloud security for web security and content management – with a unified console and policy for employees in all locations. WSGA offers TruWeb DLP for data theft and loss protection, and Advanced Classification Engine (ACE) to provide real-time security and data analysis. Websense ThreatSeeker Network inspects three billion to five billion requests from 900 million endpoints daily.

The tool offers a single management console and policy that manages defenses for office, remote and mobile users. It’s part of the TRITON solution that unifies web, email, data and mobile security across on-premise and cloud platforms for a lower cost.

ACE protects against malicious scripts and zero-day threats that circumvent anti-virus products. It analyzes web traffic in real-time, categorizing dynamic web content/threats offering detection of advanced payloads, exploited documents, mobile malware protection and much more.

Finalists 2013
• Barracuda Networks for Barracuda Web Application Firewall
• Dell SonicWALL for Dell SonicWALL SRA Web Application Firewall Service
• Fortinet for FortiWeb-400C
• IBM for IBM Security Network IPS/Network Protection
• Imperva for SecureSphere Web Application Firewall

Finalists 2013
• Barracuda Networks for Barracuda Web Security
• EdgeWave for iPrism Web Security
• Websense for Websense Web Security Gateway Anywhere
**Excellence Awards**

**BEST CUSTOMER SERVICE**

**WINNER**

*Barracuda Networks for Barracuda Customer Service and Support*

Barracuda Networks 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 our products most effective.

Barracuda Networks provides documentation that is easy to understand and is effective. In fact, *SC Magazine* conducted a review of its flagship email security offering in September 2012 and said, “We found deployment of this product to be quick and easy.”

Barracuda Networks strives to provide awesome customer service with live people always on the receiving end to help troubleshoot — there are no phone trees and no automated service.

Also, Barracuda Networks customers are provided with telephone support. Since inception, Barracuda Networks has prided itself on the “IT Guy Next Door” mentality — 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.

Too, Barracuda Networks customers 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.

Barracuda Networks customers are provided with online forums and FAQ sections online at no additional charge. Additionally, it provides Live Chat directly on the website, LinkedIn User Groups with best practice sessions, and more.

**Excellence Awards**

**BEST EMERGING TECHNOLOGY**

**WINNER**

*CipherCloud for CipherCloud Gateway*

CipherCloud is helping businesses and governments that could otherwise not adopt the cloud because of data privacy, residency, compliance and security concerns. Using real-time format and operations preserving encryption, CipherCloud ensures that customers are the only ones that can access data in the cloud while preserving the native user experience of cloud applications across browser, desktop, and mobile interfaces.

CipherCloud addresses the top six cloud computing threats as identified by the Cloud Security Alliance: insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking and unknown risk profile.

For those using the cloud, significant data privacy, residency, compliance and security challenges exist. Encryption is the most widely and universally recognized means to ensure that sensitive data remains private and always in control of the enterprise. Gartner estimates that by 2016, 25 percent of all enterprise will use a cloud encryption gateway.

CipherCloud launched its first product in February 2011. As of September 2012, CipherCloud has more than 40 large enterprise customers in production with more than one million users. This includes two of the top five U.S. banks and two of the top five Canadian banks.

CipherCloud encryption gateways are delivered as virtual appliances and can run across virtualization systems from VMware, Microsoft, and Citrix as well as IaaS platforms from Amazon, Microsoft, and Google. CipherCloud encryption gateways can quickly be enabled and disabled and scaled with simple load balancing. A production deployment supporting more than 100,000 users is deployed with two gateways always running and two more on standby to support additional load.

---

**Finalists 2013**

- Barracuda Networks for Barracuda Customer Service and Support
- eSoft for eSoft Customer Support
- Kaspersky Lab Americas for Kaspersky Business Products
- Qualys for QualysGuard Technical Support
- Vanguard Integrity Professionals for Vanguard Customer Service

---

**Finalists 2013**

- Black Lotus for Human Behavior Analysis
- CipherCloud for CipherCloud Gateway
- CloudPassage for CloudPassage Halo
- Microsoft for Enhanced Mitigation Experience Toolkit (EMET) 3.0
- Pindrop Security for Fraud Detection System
- Webroot Software for Webroot SecureAnywhere Business - Endpoint Protection
Excellence Awards

BEST ENTERPRISE SECURITY SOLUTION

WINNER
Tenable Network Security for SecurityCenter

With more than 15,000 customers, more than 1,000 of the world’s largest organizations and a community of more than one million users, Tenable is a leader in the vulnerability and compliance management market.

Its company founders are widely recognized technology leaders – CEO Ron Gula (IDS/IPS innovator), Chief Research Officer Renaud Deraison (creator of Nessus), and Chief Security Officer Marcus Ranum (developed the first commercial proxy firewall) – who spend time daily responding to questions. Tenable also provides detailed white papers, webinars, videos, and blog posts designed to help customers with detailed instructions for achieving compliance initiatives.

Tenable’s SecurityCenter has a low total cost of ownership and a rapid return on investment. The solution is quick and easy to deploy, manage and scale, and comes stocked with hundreds of prebuilt dashboards and reports that automate audits, vulnerability, attack path, threat analysis and information sharing across the organization – saving enterprises hundreds of thousands of dollars annually.

Tenable maintains one of the industry’s largest research teams, staffed by award-winning security experts delivering updated security content daily.

During 2012, Tenable introduced new features including advanced malware detection, patch and configuration management integration, and mobile device detection helping customers stay ahead of threats.

Tenable’s unique combination of vulnerability scanning, network monitoring, log and event analysis, and analytics helps customers eliminate vulnerabilities, identify attack paths and respond to attacks even from new technologies: mobile, cloud and virtual infrastructure, the fastest growing sources of theft, disruption, and compliance violations.

EXCELLENCE AWARDS

BEST REGULATORY COMPLIANCE SOLUTION

WINNER
Websense for Websense Data Security Suite

Due to the increased fines levied by agencies for non-compliance and new regulatory requirements, organizations have reprioritized their approach to audits. Organizations recognize the need for a solution that can monitor and ensure sensitive data is not transmitted to unauthorized users, while being able to walk through the incident details and generate reports for audits.

The latest report by The Corporate Board Member/FTI Consulting, “Legal Risks on the Radar,” ranked data security as the top concern of corporate America. With increasing external threats from hackers using advanced malware, organizations realize they need to account for both accidental data loss from employees and deliberate attacks from external entities. In 2011, the number of customers with Websense DLP exceeded 2,000. Websense DLP is now deployed in more than 50 countries with approximately two million users.

All customers receive specialized support from technical engineers in support centers worldwide, which regularly average 8.91 (out of 10) in satisfaction surveys. An online knowledge base, a forum of more than 19,000 individuals, technical alerts, monthly training webinars and personal myWebsense.com accounts are also available.

Websense Data Security Suite offers more than 1,600 policies and templates out of the box, many of which are regulatory requirements. These extensive built-in regulatory policies enable customers to quickly deploy the necessary controls for regulatory compliance.

With the constant release of new and updated regulations, Websense provides new regulatory policies monthly. Websense also offers a custom policy service for free, if customers are challenged with crafting a regulatory policy for their specific needs.

Finalists 2013

• CA Technologies for CA Content-Aware IAM Solution
• FireEye for FireEye Malware Protection System
• Qualys for QualysGuard Enterprise
• Sourcefire for Sourcefire Next-Generation IPS (NGIPS)
• Tenable Network Security for Tenable SecurityCenter
• Varonis Systems for Varonis Data Governance Suite

Finalists 2013

• Agiliance for Agiliance RiskVision with Agiliance Compliance Manager Application
• Qualys for QualysGuard Policy Compliance
• RSA, the security division of EMC, for RSA Archer eGRC
• Symantec for Symantec Control Compliance Suite 11
• Websense for Websense Data Security Suite
WINNER
Mandiant

Founded in 2004, and named “Best Security Company” by SC Magazine in 2012, Mandiant solutions, services and expertise set the standard in advanced threat detection and incident response. Mandiant counts more than 30 percent of the Fortune 100 as clients, many refered by law enforcement agencies.

Its products and services help guide customers through the process of detecting, responding and containing an attack. Its responders and forensic investigators are directed by the latest technical and investigative intelligence from the front lines.

Mandiant Intelligent Response (MIR) is today a leading incident response technology for combating advanced threats. The company’s MCIRT Managed Defense product combines the technology of MIR with its Computer Incident Response Team (MCIRT) whose combined experience in advanced threat detection and response, along with Mandiant’s proprietary network intelligence, provides customers with effective incident insight – from host to network – along with actionable intelligence.

The company’s R&D efforts are evidenced by eight free forensic software offerings to improve incident response and forensics technology.

In July, Mandiant announced its new research division, Mandiant Labs, to bring together reverse engineers, malware analysts and researchers onto a single team to drive innovation and automation across the company and support products and services via intelligence gathering and analysis and advanced analytics and service delivery automation.

The company offers clients training program built on real-world consultant experiences. Through incident response, malware analysis and memory forensics tracks, students learn the skills necessary to solving crime in the field.

WINNER
Kaspersky Lab Americas for Kaspersky Endpoint Security for Windows Workstations

The core challenge in today’s environment isn’t that there are no tools available, it’s that each individual tool adds to the complexity users face when trying to implement security policies. Businesses need to reduce the number of tools used and number of consoles managed, so they can get back to focusing on their core business competencies. With Kaspersky Endpoint Security 8, customers can protect data, improve overall efficiency and secure mobile computing with encryption and device management.

By combining multiple technologies into a single, centrally-managed solution, Kaspersky Endpoint Security 8 for Windows Workstations offers an extensive set of tools to ensure security and control over an array of applications, devices and web content. Kaspersky features range from a ready-to-use template to granular policy controls, all of which help administrators customize Kaspersky’s solution to their own organizations’ unique needs, thus simplifying the user experience while providing extensive security and management.

In addition to anti-malware, Kaspersky Lab’s solution manages software vulnerabilities, provides data encryption in case laptops are lost or stolen and provides security for smartphones and tablets. Kaspersky Endpoint Security 8 provides all this functionality from a single pane of glass and is built from the same code-base to work together, providing a significantly easier user experience and true value to the customer.

Kaspersky Lab continues to make major investments in R&D to develop in-house new technologies to strengthen its portfolio. All its technologies are built from the same code base and work together seamlessly, not cobbled together on the backend. The result is solutions that are more efficient and easier to manage.

Finalists 2013
- Cyber-Ark
- Dell SonicWALL
- Mandiant
- Sophos
- Sourcefire
- Verizon

Finalists 2013
- AirWatch for AirWatch Enterprise Mobile Management
- Kaspersky Lab Americas for Kaspersky Endpoint Security for Windows Workstations
- Qualys for QualysGuard Express
- Sophos for Sophos UTM 9
- SpectorSoft for SPECTOR 360
Excellence Awards

ROOKIE SECURITY COMPANY OF THE YEAR

WINNER

Pindrop Security

Originally, the belief was that Pindrop Security technology would provide call analysis for recorded calls to identify potential fraud. However, improvements to accuracy and the ability to detect specific niche cases, such as “dead air” calls and call forwards, have significantly expanded applicability to cover all areas of phone security.

The process of authenticating customers through knowledge-based authentication questions is an unsatisfactory solution. It reduces satisfaction by treating customers like criminals, and by putting the burden on them to remember secret answers, passwords and more. It increases call length, therefore adding cost. And it’s ineffective since a fraudster can find most answers to these questions online.

Pindrop Security’s technology allows companies to reduce or eliminate this process. Authentication is transparent to the customer. Detection of fraudsters is reliable and can be done prior to the call center. With Pindrop Security solutions, the call center can return to focusing on satisfied customers. Its products combine techniques to provide a multi-layered defense against fraud, using blacklisting and anomaly detection to uncover fraudsters.

Pindrop Security provides services and solutions to the largest financial institutions in the world, including systems used inline in their call centers.

Pindrop Security was founded out of research initiated at Georgia Tech’s Information Security Center (GTISC) by Vijay Balasubramaniyan (below) and the director of GTISC, Mustaque Ahamad. Balasubramaniyan is now CEO of Pindrop Security and Ahamad is chief scientist. National Science Foundation grants have continued to fund ongoing research into Balasubramaniyan’s original research, and Pindrop Security continues to grow its research in order to continually improve accuracy and capabilities of the technology.

Professional Awards

BEST CYBER SECURITY HIGHER EDUCATION PROGRAM

WINNER

Champlain College for Computer Forensics and Digital Investigation Degree Programs

Through its on-campus, online and graduate degree programs, Champlain offers more than 35 computer forensics and digital investigation courses—more than any other college in the country. Students can jump into digital forensic courses immediately, taking advantage of leading-edge courses, like mobile device forensics, network forensics, file systems forensics, and many more.

Courses are developed and taught by industry experts who bring current industry best practices and techniques to the classroom. And, its Leahy Center for Digital Investigation enables students to get to work on active investigations, gaining valuable real-world experience, including developing and writing response plans.

Champlain graduates are extremely well prepared to create and manage ever-evolving risk management plans. More than 90 percent of graduates have job offers within 30 days of graduation, and many even well before graduation.

Champlain students are highly encouraged to participate in internships and the college offers assistance in those placements. The Leahy Center for Digital Investigation hires a large number of interns to work on projects supervised by professional investigators on active cases.

This year, Champlain conducted an “Imagine College” program for under-served students. They were able to explore college as an opportunity they may not have considered to be within their reach.

(below) Champlain College President David Finney and Sen. Patrick Leahy, D-Vt., at the opening of The Patrick Leahy Center for Digital Investigation, a new Center of Excellence at the college offering students an up-to-date facility in which to learn and practice digital forensic investigation techniques.
Professional Awards

BEST PROFESSIONAL CERTIFICATION PROGRAM

WINNER
Information System Audit and Control Association (ISACA) for Certified in Risk and Information Systems Control (CRISC)

With more than 100,000 members in 180 countries, ISACA provides a vast pool of knowledge and research that is shared globally with members and nonmembers through conferences (both in-person and virtual settings), webinars, a bimonthly journal, training courses, social media groups, blogs and research publications. Additionally, ISACA offers a network of nearly 200 chapters worldwide, offering IT security professionals local training, professional networking, certification review courses and opportunities for the exchange of ideas and information. Members are also provided opportunities to take on leadership roles, participate in the development of research publications and speak at worldwide conferences. To ensure that certifica-
tion candidates demonstrate up-to-date skills, job practices for ISACA certifications are closely monitored, analyzed and updated within every five years. To determine how to best serve the IT security professional, ISACA conducts a “Member Needs” survey annually.

The CRISC certification was developed by a nonprofit, independent global leader in security, risk, governance and compliance. It provides a tool to help assess the proficiency of a professional’s IT-related risk management skills. CRISC is a highly desired certification because it is the only certification that positions IT professionals for future career growth by linking IT risk management to enterprise risk management.

Nearly 17,000 professionals across a range of job functions – including IT risk, security, audit and compliance – have earned CRISC since it was established two years ago. This number includes more than 1,200 CIOs, CISOs and chief compliance, risk and privacy officers.

Finalists 2013
- GIAC for GIAC Security Expert (GSE)
- GIAC for GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- ISACA for Certified in Risk and Information Systems Control (CRISC)
- ISACA for Certified Information Security Manager (CISM)
- ISACA for Certified Information Systems Auditor (CISA)

Professional Awards

BEST PROFESSIONAL TRAINING PROGRAM

WINNER
(ISC)² for The (ISC)² Education Program

(ISC)² delivers efficiency in certification for individuals by tapping into innovative technologies and learning strategies. (ISC)² Education Program engages current and future students and young and experienced professionals to support workforce initiatives and inspire a continuous supply of knowledgeable professionals.

Technology is evolving rapidly. (ISC)²’s Education Program reflects this change through updated review seminars. The goal is to promote and increase a candidate’s ability to retain and transfer the knowledge gained in the certification training course by improving the study material, training experience and refining performance on the job. Recent changes include measuring knowledge gain through the use of pre- and post-test analytics; restructuring course content to be both practical in knowledge needed for exam study and applicable in order to increase retention, transfer and recollection on the job; and including value-added, real-world application activities to increase motivation for learning the skills and concepts necessary for success.

The (ISC)² common body of knowledge (CBK) defines the expertise needed in a framework that provides standardized information security principles. This framework establishes a way to assess a candidate’s mastery of certain domains of knowledge and includes the most relevant, current topics of the profession today. The (ISC)² Education Program aims to change the landscape by helping professionals foster this.

Virtual and in-person security leadership events offer exclusive access (free to 86,000 members) and continuing education opportunities to industry professionals looking for timely, relevant and “hot topic” content featuring expert speakers and unique networking opportunities.

Finalists 2013
- Guidance Software for Guidance Software Training
- Inspired eLearning for Security Awareness Training
- (ISC)² for The (ISC)² Education Program
- Secure Ninja for SecureNinja Cyber Security Training Program
- The SANS Institute for SANS Training
**Professional Awards**

**BEST SECURITY TEAM**

**WINNER**

ICS-CERT Security Team for U.S. Department of Homeland Security

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Security Team responds to incidents, vulnerabilities and threats that can impact those industrial control systems (ICS) which operate critical infrastructure across the United States. These systems are vital for the processes used throughout many critical sectors that the nation depends on every day.

The ICS-CERT Security Team’s mission is to reduce cyber security risks by offering four core products and services to the nation’s critical infrastructure sectors: Providing situational awareness to government and the private sector through national alerts and advisories that warn of cyber threats and vulnerabilities; conducting technical analysis of malware, system vulnerabilities and emerging exploits; performing cyber security incident response for asset owners and operators; and partnering with the control system community to coordinate risk management efforts and serve as the focal point for information exchange.

The ICS-CERT Security Team has received national and international recognition as an essential element for coordinating cyber security risk reduction efforts among the nation’s critical infrastructure asset owners. Through its incident response, situational awareness and recommended practices efforts, the team is recognized as a national resource for cyber security guidance.

It is also a key functional element of the DHS National Cyber Security and Communications Integration Center (NCCIC) and is integral to the department’s capability to coordinate national-level cyber events. ICS-CERT Security Team presence in the NCCIC Operations Center provides synergistic information-sharing value to the various public and private sector partners.

**WINNER**

The ICS-CERT Security Team has received national and international recognition as an essential element for coordinating cyber security risk reduction efforts among the nation’s critical infrastructure asset owners. Through its incident response, situational awareness and recommended practices efforts, the team is recognized as a national resource for cyber security guidance.

It is also a key functional element of the DHS National Cyber Security and Communications Integration Center (NCCIC) and is integral to the department’s capability to coordinate national-level cyber events. ICS-CERT Security Team presence in the NCCIC Operations Center provides synergistic information-sharing value to the various public and private sector partners.

**BEST SECURITY TEAM**

**Finalists 2013**

- Go Daddy Security Team
- Teleperformance Security Team

---

**Professional Awards**

**CSO OF THE YEAR**

**WINNER**

John South, CSO, Heartland Payment Systems

John South has established a best-in-class IT security team at Heartland Payments Systems by hiring the most talented practitioners to manage the various elements defined in the security program. Seeking team members that have strong communicative and technical capabilities, he stresses the importance of compatibility between the company’s risk/needs and individuals’ strengths.

Once team members are identified and on-boarded, South ensures they have ample opportunities to continually expand their knowledge with access to a variety of security training resources. Further, South challenges his team members to grow their expertise by pursuing professional development opportunities. He encourages his staff to earn both CISSP and CISA credentials, as well as at least one additional expertise-specific certification.

With this foundation, South empowers his team to take ownership of security initiatives and lead the application of security principles and guidelines to mitigate risks that face the enterprise.

By aligning Heartland’s security program with the company’s corporate objectives, South and his team have won the support of corporate leaders and colleagues. In doing so, South has established the business of security at Heartland as a vehicle to support the organization’s various business units.

Coming to the table with solutions that help leaders securely accomplish their objectives, and being able to effectively communicate these measures, South and his team have solidified their roles as true business partners for groups across the organization. Looking out for the best interests of business units and merchant customers, South and his staff have earned respect and even converted once-skeptical business leaders into internal champions for the group.

**Finalists 2013**

- Bobby Dominguez, director, IT security and GRC, PSCU Financial Services
- Nikk Gilbert, vice president and chief information security officer, CUNA Mutual Group
- John South, CSO, Heartland Payment Systems
- Bruce Wignall, CISO, Teleperformance

---
Professional Awards

**EDITOR’S CHOICE**

**WINNER**
Electronic Frontier Foundation (EFF)

In an environment that primarily measures achievement in net sales or visibility, it’s particularly rewarding for us to call out the work of an organization that can prioritize ideals – particularly privacy protection in our new age of digital connectivity.

The nonprofit Electronic Frontier Foundation (EFF) takes on those who hold the reins – whether in government or industry – large, intimidating forces which, and can often, abuse their privilege, such as in overzealous prosecutions, as was just evidenced in the case of Aaron Swartz. The EFF has put its weight behind Aaron’s Law, a proposed update to the Computer Fraud and Abuse Act that, among other principles, aims to make certain that questionable innovations are not treated as criminal offenses and that penalties are proportionate to allegations of wrongdoing.

Another initiative the technology watchdog group has recently undertaken is the Coders’ Rights Project. This effort aims to safeguard programmers and developers as they perform their work. As many of these security and encryption researchers come up against a slew of state, federal and international legal limitations, the EFF advocates that the momentum of these innovators should not be hindered. On their behalf, the group – which maintains an active presence at conferences, like Black Hat and DefCon – promotes education, stands ready to prepare legal defenses and carries on public programs to ease the path forward for technological innovation, including the work of hackers and others on the edges of digital exploration. In addition, the group has a presence on Capitol Hill, providing policy advice to legislators involved in deciding new computer crime legislation.

The group’s advocacy for privacy protections extends into many areas touching technological progress. Just last month, the EFF filed an amicus brief in a Maryland case to voice its concern about the collection of DNA from those arrested for a crime, insisting that warrants must be served by law enforcement before anyone is required to provide a genetic sample. The point, it argued, is that the accessibility of advanced technology should not undermine traditional privacy protections.

Further, last year, the group began a project to delve into the certificates in use to secure all of the sites encrypted with HTTPS on the web. The goal of the EFF SSL Observatory, aided by a substantial gift from entrepreneur Mark Cuban and game developer Markus Persson, is to uncover vulnerabilities; substantiate the practices of certificate authorities, the organizations delegated to sign cryptographic certificates trusted by browsers; and help those further developing the underlying encryption infrastructure of the web.

Too, the EFF recently became involved in a case in San Francisco that pitted a group of Reddit “gaymers” – members of the lesbian, gay, bisexual, and transgendered community active in video games – against a website operator who had registered the term as a trademark. The trademark registration should be canceled, the group stated in its petition to the U.S. Patent and Trademark Office, so that the term can be used worldwide. The EFF, in association with the law firm Perkins Coie, is backing up the gaymers, arguing that the term had been in use for several years prior to the adversary’s claim and therefore belongs in the public domain.

“Trademarks have one primary purpose: To protect consumers from confusion about the source of goods or services,” said EFF Staff Attorney Julie Samuels at the time of the filing. “This registration isn’t being used to protect consumers – it’s being used to threaten free speech.”

Whether it is there with an argument for what it believes is a dangerously narrow view of fair use, or debating in court with police departments to challenge the use of invasive technology, such as GPS tracking devices on a suspect’s car, the EFF stands up to the overseers – alleged and in place – to insist that powerful interests must not shun the rule of law. In doing so, it smooths the path for technological innovation and those whose thinking outside the box transgresses ordinary boundaries that only serve the privileged and powerful.