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 phishing, custom malware and targeted attacks are happening at a rate never witnessed before, a data-centric approach to security now is 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. — Illena Armstrong, VP, editorial, SC Magazine
2013 SC Awards U.S.

The Judges

CO-CHAIR
Ilenna Armstrong
VP, editorial, SC Magazine

CO-CHAIR
Rich Baich
CISO, Wells Fargo

Philip Apcasilli
CISO, Cox Communications

Rebecca Bace
CEO, Infield

Jennifer Bayuk
principal, Jennifer L. Bayuk, LLC

Bruce Bonsall
senior security strategist, BT US&C

Dennis Brixius

Chris Camacho
information security officer, The World Bank

Jaime Chanaga
CEO, The CSO Board

Rafael Diaz
CSO, 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
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

2013 SC Awards U.S.

The Sponsors

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

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

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

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

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

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

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

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

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

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

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

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

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.

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 trade craft 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 basic common sense 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 appreciate your partnership in dealing with the unprecedented threats we all face every day.

--- Rich Baich, co-chairman, 2013 SC Awards U.S.; CISO, Wells Fargo

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.

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.

Further vGW offers granular customer resource isolation, layers of protection, superior performance and regulatory compliance mechanisms that help users trust 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.

Finalists 2013

• Dell SonicWALL for Dell SonicWALL TZ 215
• McAfee for McAfee Web Protection
• Symantec for Symantec Web Gateway
• TrendMicro for Secure Web Gateway
• TRITON Security Gateway from TRITON Security Gateway Anywhere

Finalists 2013

• IBM for IBM Cloud Security Services
• Juniper Networks for vGW Virtual Gateway
• Sophos for Sophos SafeGuard 6
• Symantec for Symantec OV Cloud Identity and Access Control
• Trend Micro for Trend Micro Deep Security 9
• TRITON Security Gateway from TRITON Security Gateway Anywhere

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 management (SIEM) for automatic 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 efficiency 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.
book, 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 spreading 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 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 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 Face-
The Risk Engine works behind profiling and data feeds from behavioral analysis, device Authentication monitors and identity and cost. Powered by the risk-based authentication and user experience. Available

• Symantec for Symantec Code Signing
• CA Technologies for CA RiskMinder

As organizations migrate drastically improve security and efficiency. Finally, offering a solution that does not require tokens or extra passwords represents their organizational structure to defining and enforcing unique business policies to cost effectively extend automated provisioning to applications and policies.

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 compliances 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 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 – from leveraging standardized processes to detecting 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.

The MAG Series Junos Pulse Gateways 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 granular access control. The Juniper Networks MAG Series Junos Pulse Gateways dramatically improves the security posture 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 organization structure to defining and enforcing unique business and regulatory policies to cost effectively extend automated provisioning to applications and policies.

As a risk and policy-based Access Control System, the Check Point IPS Software Blade dramatically reduces the complexity of customer network security infrastructure by reducing their hardware footprint, rack space, cabling, and cooling, as well as power consumption.

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.

The Best IPsec/SSL VPN category recognizes devices and services that provide secure remote access and/or internal network connectivity via SSL VPN, MAG Series gateways or other virtual private network technology. The award recognizes products that provide comprehensive security, granular access control and threat prevention. The Juniper Networks MAG Series Junos Pulse Gateways dramatically improve the security posture 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 organization structure to defining and enforcing unique business and regulatory policies to cost effectively extend automated provisioning to applications and policies.

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 – from leveraging standardized processes to detecting 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, and cooling, as well as power consumption.

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.
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. 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 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 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.

Finalists 2013
- Dell SecureWorks for Dell SecureWorks Managed Security Services
- IBM for IBM Managed Security Services
- Mandiant for MCIBT Managed Defense
- VeriSign for VeriSign Malware Detection
- Verizon Business for Managed Security Services – Commercial

Finalists 2013
- AirWatch for AirWatch Enterprise Mobile Management
- AVG for AVG AntiVirus FREE for Android
- Marble Security (formerly IronKey) for Marble Access
- Sophos for Sophos Mobile Control 2.5
- Symantec for Symantec Mobile Management Suite

Verizon Managed Security Services

Verizon Business for Managed Security Services - Commercial

2013 SC Awards U.S.

2013 SC Awards U.S.
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 state, 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 1,300 customers to search and investigate, proactively monitor user and machine behavior, perform statistical analysis to identify anomalies and unknown threats, and create dashboards and visualization for executives. Splunk’s architecture makes all machine data in an organization understandable 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 search for SIEM use cases.

Splunk can ingest any type of machine data from any source, whether from files, a syslog, 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 features as 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-based, heuristic, and HEIP-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 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.

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 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 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 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 TrueWeb 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 and threats offering detection of advanced payloads, exploited documents, mobile malware and much more.

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 Customer Service 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 trouble shoot – 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 issue 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 custom ers are provided with online forums and FAQ sections 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 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. Gardner 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 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

Finalists 2013
• Barracuda Networks for Barracuda Customer Service and Support
• Soft-Shell 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 Hale
• Microsoft for Enhanced Mitigation Experience Toolkit (EMET) 3.0
• Pinchsoft for Fraud Detection System
• Webroot Software for Webroot SecureAnywhere Business - Endpoint Protection

Finalists 2013
• Best Web Application Firewall
• Best Web Content Management Product
• Best Customer Service
• Best Emerging Technology

Finalists 2013
• Websense for Websense Web Security Gateway Anywhere
• Barracuda Networks for Barracuda Web Application Firewall

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 Ress Gulia (IEDS/IPS innovator), Chief Research Officer Renaud Deraison (creator of Nessus), and Chief Security Officer Marcus Rassam (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 incident response technologies 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. Kaspersky Lab’s proprietary network monitoring and investigative intelligence provides customers with the skills necessary to solve the most demanding advanced threat detection and response applications.

Excellence Awards  
BEST SECURITY COMPANY

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 10 percent of the Fortune 100 as clients, many referred 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.

Excellence Awards  
BEST SME SECURITY SOLUTION

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 bringing 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, simplify 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 new house 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
- CA Technologies for CA Content-Aware IAM Solution
- FireEye for FireEye Malware Protection System
- Qualys for QualysGuard Enterprise
- Snytefret for Sourcefire Next-Generation IPS (NGIPS)
- Tenable Network Security for Tenable SecurityCenter
- Tanium Systems for Tanium Data Governance Suite

Finalists 2013
- CyberArk
- Dell SonicWALL
- Kaspersky Lab Americas for Kaspersky Endpoint Security for Windows Workstations
- Qualys for QualysGuard Express
- Sophos for Sophos UTM 9
- SpectroSoft for SPECTOR 360

Finalists 2013
- Appliance for Appliance RiskVision with Appliance 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
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 fraudsters as unwanted callers, using challenging and anomalous detection to uncover fraudsters. Pindrop Security provides services and solutions to the largest financial institutions in the world, including systems used in their call centers.

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

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 projects supervised by professional investigators on active cases.

This year, Champlain conducted an “Imagine College” program for underrepresented students. They were able to explore college as an opportunity they may not have considered before, and as a year-end opportunity, the college offering students an “Imagine College” program underrepresented students, 11 of 15 were accepted for the program.

The Leahy Center is named for 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 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.

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 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.

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 Wagnall, CSIO, 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 turns the spotlight of attention, 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 bill to update 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 has built 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 tasked with determining new computer crime legislation. The group’s advocacy for protection extensions 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 involved in deciding new computer crime legislation. The group’s advocacy for 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.

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 has built 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 tasked with determining new computer crime legislation. The group’s advocacy for protection extensions extends into many areas touching technological progress.

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 Samuel at the time.

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 Samuel at the time.

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 tasked with determining new computer crime legislation. The group’s advocacy for protection extensions 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.

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 has built an active presence at conferences, like Black Hat and...