AWARDS 2015

Honored in the U.S.

April 21, 2015 • San Francisco

Celebrating your efforts

Even nimble security pros can only be so crafty when the majority of CEOs and boards of directors don't really want to hear about the fast-growing intensity of cyber threats. According to the recently released survey, "2015 Global Megatrends in Cybersecurity," conducted by Ponemon Institute, 78 percent of senior IT leaders responding say they hadn't briefed their boards on corporate IT security strategies in the last year.

The executives and directors should be better informed because breaches are not only an expense to operations, but a threat to their business. No board wants to see their company in the headlines as a consequence of an attack and subsequent loss of data. While not easy to calculate, brand damage can have a devastating impact on an operation – witness the fallout to just a recent spate of victims: Anthem, JPMorgan Chase, Sony, Target, Home Depot.

Yet the necessity to find more pros armed with both business and IT security acumen is hitting at the same time that most in the IT security arena are acknowledging a soon-to-be desperate shortage of pros to hire. Combine this with a consistently high turnover rate of qualified personnel and this challenge to build more solid and expert teams becomes even more complex.

SC Awards U.S. strives to help here by acknowledging the indefatigable efforts of IT security practitioners, as well as the rookie and long-standing product and service providers that support risk management plans and everyday endeavors by calling out outstanding achievements. In June, the SC Awards U.K. will be doing the same for organizations and IT security leaders in Great Britain and Europe.

It's a small contribution we've been making to the industry for nearly 20 years that enables us to draw attention to IT security and its leading players. This week's SC Awards gala in San Francisco – and the other fast-approaching in the U.K. – will show IT security pros like you some love. Survey results show y'all could use some. Meantime, I welcome your suggestions on other categories we can consider adding to our SC Awards programs.

– Illena Armstrong, VP, editorial, SC Magazine

SC MAGAZINE AWARDS 2015
Honored in the U.S.

Contents

EDITORIAL
VP, EDITORIAL Illena Armstrong
ASSOCIATE EDITOR Teri Robinson
MANAGING EDITOR Greg Masters
SENIOR REPORTER Danielle Walker
REPORTER Adam Greenberg
CONTENT COORDINATOR Robert Abel
EDITORIAL ASSISTANT Ashley Carman

2015 SC AWARDS U.S.
EVENTS DIRECTOR Adele Durham
EVENTS MANAGER Maggie Keller
ASSOCIATE VIRTUAL EVENTS MANAGER Jourdan Davis
VIRTUAL EVENTS COORDINATOR Anna Jurgowski

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
PRODUCTION MANAGER Krassi Varbanov

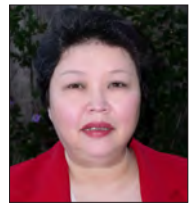
MANAGEMENT
CEO, HAYMARKET MEDIA Lee Maniscalco
CFO Donna Santarpia
COO John Crewe

U.S. SALES
VP, SALES David Steifman (646) 638-6008
EAST COAST SALES DIRECTOR Mike Shemesh (646) 638-6016
WEST COAST SALES DIRECTOR Matthew Allington (415) 346-6460
EVENT SALES DIRECTOR Mike Alessie (646) 638-6002
MARKETING DIRECTOR Karen Koza (646) 638-6169

The Judges

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

CO-CHAIR
Greg Bell
principal, KPMG and U.S. leader, KPMG Cyber



Becky Bace
chief strategist, Center for Forensics, Information Technology & Security, University of South Alabama

Rich Baich
EVP/CISO, enterprise technology services, Wells Fargo & Company

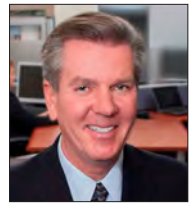
Ron Baklarz
CISO, export control compliance officer, AMTRAK

Stephanie Balaouras
VP and research director, security and risk, Forrester

Miki Calero
CISO, state of Ohio

Chris Camacho
SVP/global information security, Bank of America

Troy Donnelly
global head of information security, WorleyParsons



Thomas Dunbar
SVP, chief information risk officer, XL Global Services

Patty Edfors
VP, information security and compliance, Sirius XM Radio

Mike Fabrico
principal systems security specialist, NASDAQ

Pamela Fusco
CISO, Apollo Group

Zouhair Guelzim
CISO, L'Oréal USA

Michael Higgins
CISO, NBC Universal

John Johnson
global security strategist, John Deere

Phil Lambert
associate director, network security architecture, Starwood Hotels & Resorts Worldwide

Bob Maley
founder & principal, Strategic CISO

Bill Malik
CEO and founder, Malik Consulting

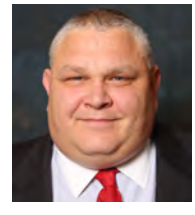
Scott Pearce
CISO, Frederick County Government

Jim Routh
CISO, Aetna

Randy Sanovic
owner, RNS Consulting

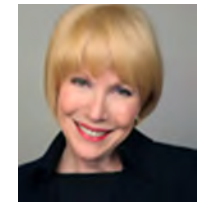
Kurt Sauer
director, governance and operations, Paypal

Howard Schmidt
partner, Ridge Schmidt Cyber



Richard Starnes
CISO, Kentucky Health Cooperative

Richard Stiennon
chief research analyst, IT-Harvest



Jody Westby
CEO, Global Cyber Risk

Larry Whiteside Jr.
CISO, Lower Colorado River Authority

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

Drew Williams
president, CEO, Condition Zebra

The Sponsors

SC Magazine thanks all sponsors for their generous support of the 2015 SC Awards U.S. Their involvement has made possible this event, which helps raise professional standards in the information security industry worldwide.

Barracuda

barracuda.com

Barracuda provides cloud-connected security and storage solutions that simplify IT.

Champlain College

champlain.edu

Champlain College offers an innovative approach to education in business, cybersecurity, digital forensics, information technology, and more.

Entrust Datacard

entrust.com

Entrust Datacard offers solutions for trusted identities and secure transactions. The company serves customers in 150 countries.

ForeScout

forescout.com

ForeScout enables organizations to continuously monitor and mitigate security exposures and cyberattacks.

HP Atalla Information Security & Encryption

HP.com/go/Atalla

HP Atalla solutions ensure protection of an organization's most sensitive information.

ISACA

isaca.org

ISACA helps business and IT leaders build trust and value from information and information systems.

LogRhythm

logrhythm.com

LogRhythm empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyberthreats.

MSLGROUP

mslgroup.com

MSLGROUP is Publicis Groupe's strategic communications and engagement group, advisers in all aspects of communication strategy.

NetHawk Interactive

nethawk.net

NetHawk Interactive is a B2B marketing and media-buying agency exclusively serving the information technology community.

Network Box USA

networkboxusa.com

Network Box USA was formed in response to increasingly sophisticated threats stemming from widespread use of the internet.

Qualys

qualys.com

Qualys is a leading provider of cloud security and compliance solutions with more than 6,700 customers in more than 100 countries.

Splunk

splunk.com

Splunk software searches, monitors, analyzes and visualizes Big Data from websites, applications, servers, networks, sensors and mobile devices.

Trend Micro

trendmicro.com

Trend Micro security solutions protect information on mobile devices, endpoints, gateways, servers and the cloud.

Veracode

veracode.com

Veracode's cloud-based service and programmatic approach deliver a simpler and more scalable solution for reducing global application-layer risk.

Welcome from the co-chairman

When considering the state of information security over the past 14 months, the most effective description I can provide is: "game-changing." The threats we are facing from an increasingly sophisticated set of adversaries, continues to evolve at an unprecedented rate. The impact to our businesses and organizations has reached the highest level of importance and perspective. The expectations of our customers, our business partners and our governments are similarly at all-time highs.

In this country alone, we've seen large amounts of our financial and health-care information stolen and exploited by cybercriminals. We've seen devices being wiped of all data resulting in productivity losses. We've seen personal and professional reputations damaged by disclosure of private communications. There is nothing in the foreseeable future that would predict that the pace or nature of these incidents will diminish.

Amongst this backdrop of evolving risk, our businesses – and the technologies we deploy to support them – are similarly changing as our economies and transactions become more mobile, more social and more personal. These divergent needs – to balance rapid business growth with increasingly more sophisticated technical risks – requires a new set of players for the new game that is evolving around us.

To be successful, the information and cybersecurity disciplines require a new type of practitioner: one driven by innovation, leadership and passion. We require information security leaders who can efficiently navigate through the political and fiscal challenges that must be continually faced at the organizational and governmental levels. We need technical innovators who can identify the new avenues of threats, and then rapidly develop solutions to prevent, detect or react against these threats. We need passionate and dedicated teams of practitioners who work tirelessly to protect their countries and their organizations.

The 2015 SC Awards U.S. are here to celebrate those players who help us play this new game more effectively every day. They represent the very best of innovation, of leadership and of passion. I'm very proud to partner with *SC Magazine* to help select and honor all of the incredibly innovative nominees and those visionaries who will be recognized as the leaders over tonight's categories. Thank you all for what you do!

Greg Bell
principal, KPMG and U.S. leader, KPMG Cyber

Reader Trust Award

BEST ADVANCED PERSISTENT THREAT (APT) PROTECTION

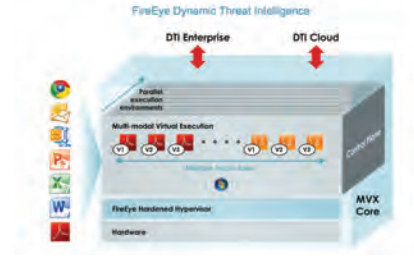
WINNER

FireEye for FireEye Threat Prevention Platform

The FireEye platform combats today's advanced cyber attacks and is designed from the ground up to stop advanced persistent threats used by cybercriminals. With the FireEye Threat Prevention Platform, Dynamic Threat Intelligence, and Services, enterprises get multifaceted defense capabilities to guard against sophisticated attacks including zero-days, unknown malware and APT attacks.

The core of the FireEye platform is the patented Multi-Vector Virtual Execution (MVX) engine, which provides dynamic, signature-less and virtualized analysis of today's advanced cyber attacks. The core of MVX begins with the FireEye hardened hypervisor, a purpose-built hypervisor designed for threat analysis with built-in countermeasures against malware. The MVX engine detonates suspicious files, web pages and email attachments within instrumented virtual machine environments to confirm a cyber attack. This threat intelligence is in a standards-based format, which enables the intelligence to be correlated and shared among the entire FireEye deployment to stop today's cyber attacks.

FireEye offers the breadth and depth of signature-less protection across a range of zero-day APT attacks and attack methods. The Multi-Vector Virtual Execution engine is extensible to multiple threat vectors to address web, email, mobile and content-based attacks enabling correlation across attack vectors, and provides security at multi-gigabit speeds to protect at scale. FireEye enables consolidation of IT resources, lowering the total cost of threat prevention. It is built with a custom hypervisor with built-in countermeasures and malware detection that extends to endpoints.



Finalists 2015

- Check Point Software Technologies for Check Point Threat Prevention
- Cisco for Cisco Advanced Malware Protection
- **FireEye for FireEye Threat Prevention Platform**
- Palo Alto Networks for PA-7050 Next-Generation Firewall
- Trend Micro for Trend Micro Deep Discovery

Reader Trust Award

BEST CLOUD COMPUTING SECURITY SOLUTION

WINNER

Blue Coat Systems for Blue Coat Cloud Security Solution

Blue Coat's cloud-based services allow enterprises to enhance employee productivity and deliver cost savings by removing the need of on-premise hardware and software. Blue Coat safeguards the processing of an organization's data across all its cloud service offerings. As with the Industrial Revolution, cloud computing or software-as-a-service (SaaS), has accelerated information consumption and impacted the speed of innovation.

Today, the cloud has also enabled the enterprise to extend its corporate security perimeter to all devices in any location and deliver the same performance benefits as if it was on premise. Blue Coat's Global Cloud Infrastructure provides fast, easy deployment and scalability so enterprises can seamlessly deploy it within an existing security framework and scale on-demand to support new user requirements.

Blue Coat's Cloud Web Security Service provides proactive web protection to organizations of all sizes without updating appliances, servers or user desktops – meaning no disruption to the normal work day. It uses Blue Coat WebPulse, which integrates threat intelligence data from more than 75 million end-users to create a collaborative defense mechanism ensuring real-time protection against threats.

With extensive web application controls and detailed reporting features, administrators can create and enforce policies that are instantly applied to all covered users, including fixed locations and roaming users.

Blue Coat stands out because of its combination of collaborative defense and security technology, which empowers businesses to focus on other revenue-generating projects.

Finalists 2015

- AirWatch by VMware for AirWatch Enterprise Mobility Management
- **Blue Coat Systems for Blue Coat Cloud Security Solution**
- Dell Software for Dell One Identity Cloud Access Manager
- Juniper Networks for Firefly Perimeter
- Trend Micro for Trend Micro Deep Security

Reader Trust Award

BEST COMPUTER FORENSIC SOLUTION

WINNER

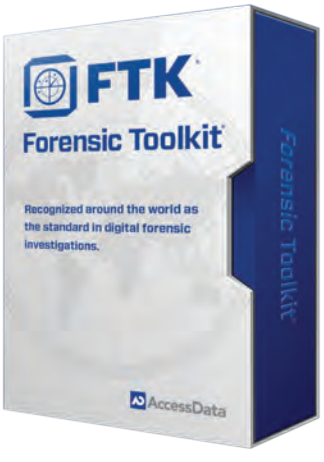
AccessData Group for Forensic Toolkit (FTK)

Forensic Toolkit (FTK) is recognized around the world as a leading standard in computer forensics software. It is a court-cited digital investigations platform built for speed, stability and ease of use. It provides comprehensive processing and indexing up front, so filtering and searching is faster than with any other product. This means users can zero in on the relevant evidence quickly, dramatically increasing their analysis speed. The database-driven, enterprise-class architecture allows users to handle massive data sets, as it provides stability and processing speeds not possible with other tools. Because of this architecture, FTK can be upgraded easily to expand distributed processing and incorporate web-based case management and collaborative analysis.

A First Look review in *SC Magazine* last year said, "FTK has been our workhorse for several releases. It always has provided the power we need and the speed that makes processing large cases practical." FTK differs from the competition for several reasons, including its database-drive design, interoperability with other AccessData's solutions, its data processing speed, its ability to remotely analyze and acquire computers, as well as the fact that it can be expanded to include malware analysis. Because it's database-driven, users can avoid the frequent crashing and lost work associated with memory-based tools. It provides the most comprehensive processing at speeds that are unmatched by other solutions. Clients have reported their ability to comprehensively process more than a terabyte of complex data in 12 hours. Finally, the remote investigation capability, malware analysis and visualization tools make FTK a more comprehensive solution that enables a more efficient and thorough investigation process.

Finalists 2015

- **AccessData Group for Forensic Toolkit (FTK)**
- FireEye for FireEye Network Forensics Platform
- Guidance Software for EnCase Forensic
- LogRhythm for LogRhythm's Network Monitor
- Rapid7 for UserInsight



Reader Trust Award

BEST DATA LEAKAGE PREVENTION (DLP) SOLUTION

WINNER

General Dynamics Fidelis Cybersecurity Solutions for Fidelis XPS

Data theft protection is a problem that requires awareness of the entire threat lifecycle in order to stop data exfiltration at any phase that it occurs. Fidelis XPS is a comprehensive advanced threat defense solution that stops targeted attacks and the resulting data theft across all phases of the threat lifecycle, including initial infiltration via commodity or advanced targeted malware, command-and-control communication, lateral propagation and the resulting data exfiltration. Fidelis XPS is specifically designed to detect and prevent threats against data loss by monitoring network traffic – including all protocols and applications – with patented Deep Session Inspection, providing real-time, bi-directional protocol, application and content decoding and analysis. Fidelis XPS combines advanced malware protection, network security analytics and data theft protection in a single, tightly integrated system for continuous protection across the enterprise with maximum awareness of threats against corporate sensitive data, intellectual property, business plans, etc.

Fidelis XPS takes a unique approach to DLP by unifying advanced threat protection (the attack mechanics), network security analytics (content-infused metadata) and data theft protection into a single, tightly integrated system for continuous monitoring and protection across the enterprise. Fidelis XPS's Deep Session Inspection technology exposes, extracts and analyzes malware hidden in all network protocols, applications and content types. This unparalleled visibility allows for detection and prevention across all phases of the threat lifecycle.

Additionally, Fidelis XPS's flexible policy engine allows security analysts to block data exfiltration by configuring protection mechanisms to match the organization's data profile.

Finalists 2015

- AirWatch by VMware for AirWatch Secure Content Locker
- Check Point Software Technologies for Check Point DLP Software Blade
- **General Dynamics Fidelis Cybersecurity Solutions for Fidelis XPS**
- McAfee for Data Loss Prevention (DLP)
- Varonis Systems for Varonis IDU Classification Framework
- Websense for Websense TRITON AP-DATA + AP-ENDPOINT

Reader Trust Award

BEST DATABASE SECURITY SOLUTION

WINNER

HP Atalla for HP Enterprise Secure Key Manager with HP Secure Encryption

Many companies, especially those subject to industry regulations, require sensitive data to be secured against threats like unauthorized insider access, accidental disclosure and theft. Auditors, regulators and industry compliance mandates often require encryption of sensitive data at rest as a minimum standard of security best practice. HP Enterprise Secure Key Manager (ESKM) provides a complete solution for unifying and automating an organization's encryption controls by securely creating, protecting, serving, controlling and auditing access to encryption keys. When sensitive data at rest is encrypted, the risks of audit failures, financial losses and damage to an organization's reputation are significantly reduced. Data at rest requires strong key management practices with policy enforcement to manage, protect, serve and preserve underlying encryption keys over the life of the data. HP Secure Encryption, combined with HP Smart Array controller-based data encryption for HP ProLiant Gen 8/Gen 9 servers, protects data at rest on bulk storage.

HP is a leading provider of security and compliance solutions that mitigate risk for hybrid environments and defend against advanced threats. HP ESKM is designed as a fully integrated solution, supporting a broader range of encryption solutions than its competitors and scaling easily to eight-node distributed geographic clusters for more than 20,000 enrolled clients and more than two million keys. Additionally, every ESKM release has been validated to a FIPS 140-2 Level 2 rating. Standard capabilities include high availability clustering and failover, secure key database, key generation and retrieval services, identity and access management, secure backup and recovery, a local Certificate Authority and strong audit logging for compliance validation.

Finalists 2015

- DB Networks for DB Networks DBN-6300
- GreenSQL for GreenSQL Database Security and Compliance
- **HP Atalla for HP Enterprise Secure Key Manager with HP Secure Encryption**
- Trustwave for Trustwave DbProtect
- Vormetric for Vormetric Data Security Platform

Reader Trust Award

BEST EMAIL SECURITY SOLUTION

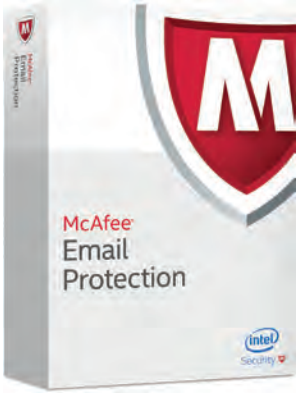
WINNER

Intel Security for McAfee Email Protection

McAfee Email Protection combats targeted phishing attacks and advanced malware, while preventing data exfiltration (compliance and data privacy). McAfee has been chosen by some of the largest enterprises in the world to defend against the most sophisticated malware attacks and targeted phishing, to keep their employees productive and to eliminate sensitive data exfiltration via email. Organizations are empowered to mature their email security practice with advanced technologies – such as encryption and data loss prevention – built into the product and available when the customer is ready. McAfee email security customers span all market segments from financial services, manufacturing, retail, transportation, health care and government agencies. These customers appreciate McAfee's dedicated focus to breadth of security solutions.

As customers consider moving their inboxes to the cloud over the next refresh cycle, McAfee enables them to take the same enterprise-grade security to those mailboxes at no additional charge. This enables ultimate flexibility for customers to test and migrate mailboxes in a phased approach without compromise. Single end-to-end email security and flexible any-form-factor at any-time licensing frees up IT to focus on strategic activities. The solution eliminates cycles of procurement, deployment, integration and on-going maintenance of various products to address in-bound and data extrusion security. And, it supports those looking to move to hosted mailboxes.

As a leading source for threat research, threat intelligence and cybersecurity thought leadership, McAfee Labs' team of 500 researchers correlates real-world data collected from millions of sensors across key threat vectors. This visibility of the landscape delivers intelligence to email security to increase protection and reduce risk.



Finalists 2015

- Barracuda for Barracuda Email Security Service
- Cisco for Cisco Email Security Appliance
- **Intel Security for McAfee Email Protection**
- Proofpoint for Proofpoint Enterprise Protection/Privacy
- Websense for Websense TRITON AP-MAIL

Reader Trust Award

BEST FRAUD PREVENTION SOLUTION

WINNER

Splunk for Splunk Enterprise

As more business moves online, the patterns of fraud, theft and abuse are often found in an organization's machine data or log files, just as the patterns of an advanced cybersecurity threat are often revealed in machine data. Authentication systems, firewalls, databases, billing and other systems all generate machine data, which likely contain the subtle patterns of fraud when and where fraud exists.

Splunk, used by more than 7,900 global customers, is a Big Data platform that can index any type of machine or log data without up-front normalization and at massive scale. This data can then be searched, correlated, alerted and reported on in real-time for a wide range of anti-fraud use cases, including fraud investigations, detection, prevention and reporting. Because Splunk is a highly flexible platform, anti-fraud teams can use it to quickly adapt to changing fraud techniques and to address a wide range of team needs.

Splunk can index any type of machine data or log files from any source and retain all the original data for searching and reporting. Splunk also leverages a flexible search language that enables a wide range of searches and visualizations, including the detection of outliers and anomalies that might be fraud.

Splunk uses a distributed architecture with a flat file data store and no centralized database that could slow performance. It uses distributed search technology for fast searching. It can index 100TB+ of data a day and return search results in seconds. Splunk is a unified solution with a single platform, user interface and data store.

The installation is fast and the user interface is intuitive. Thus, time to value is quick and minimal resources are needed to deploy and use Splunk.

Finalists 2015

- Entrust for Entrust TransactionGuard
- F5 Networks for F5 WebSafe/MobileSafe
- Kaspersky Lab for Kaspersky Fraud Prevention
- RSA, the security division of EMC, for RSA Web Threat Detection
- **Splunk for Splunk Enterprise**

Reader Trust Award

BEST IDENTITY MANAGEMENT SOLUTION

WINNER

CA Technologies for CA Identity Manager

Users with excessive or inappropriate privileges can potentially wreak havoc, including violating compliance mandates or causing leakage of confidential data. Automating processes for granting and verifying application access based on each user's relationship and role within the organization – whether they are employees, administrators, contractors, customers or business partners – improves IT flexibility. It also helps to improve operational efficiencies and reduce security risks by on-boarding new users faster and ensuring that all users only have access that is appropriate to their job function.

CA Identity Manager provides the ability to manage and govern user identities (including shared, administrative accounts) and answers the question, "Who has access to what?" in a simple and cost-effective manner. CA Identity Manager provides the ability to manage and govern user identities across physical, virtual and cloud environments. Designed to be easy to use and cost-effective, CA Identity Manager can help improve efficiency, security and compliance throughout the enterprise.

CA Identity Manager provides several utilities (PolicyXpress, ConfigXpress and ConnectorXpress) to help simplify management and configuration of its Identity Manager environment. ConnectorXpress lets customers build their own connectors to common types of applications without having to write code, and PolicyXpress allows configurations rather than customizations to provide workflow and policy updates.

CA Identity Manager comes with a broad set of out-of-the-box connectors (40+) from mainframe to SaaS applications. The offering also provides a mobile application (for iOS and Android) that enables users and administrators to interface with a wide range of identity management functionality from the convenience of a mobile device.

Finalists 2015

- **CA Technologies for CA Identity Manager**
- Centrify for Centrify Server Suite
- Dell Software for Dell One Identity Manager
- NetIQ for Identity Manager 4.5
- RSA, the security division of EMC, for RSA Identity Management and Governance (formerly known as RSA Aveksa)

Reader Trust Award

BEST MANAGED SECURITY SERVICE

WINNER

Dell SecureWorks for Managed Security Services

The information security market is flooded with various technology tools to protect a company's IT infrastructure from intrusions by threat actors. But these are point solutions and most companies that buy these new technologies don't have the expertise to operate them correctly. Dell SecureWorks manages and monitors security devices 24/7/365 for 3,800 clients globally. It is vendor agnostic and can manage and monitor most any device. Dell is an extension of an organization's security team, filling resource gaps and providing recommendations and expert guidance based on its global visibility into the threat landscape. Using intelligence from its Counter Threat Unit (CTU) security research group on the latest exploits and attack methods, its device engineers finetune signatures to maximize detection capabilities in the customer network, often outperforming the signatures from the device manufacturer. Based on CTU intelligence on emerging threats and information gathered from customer network changes, Dell continually tunes managed devices.

Security is all Dell does. Defending clients since March 1999, it supports clients in more than 70 countries around the world. Every call to its SOC is handled by one of its certified, experienced security professionals. Dell leverages threat intelligence that it has gathered from clients around the world, as well as intelligence it gathers from its targeted threat hunting and IR services. What makes Dell different from other MSS companies is that clients hear from the company as often as anything suspicious gets through their networks. Dell puts its monitoring device in prospects' businesses for 30 days and have a feed going to it while the client is still being monitored by its current MSS company.

DELL SecureWorks

Finalists 2015

- Cisco for Managed Threat Defense
- **Dell SecureWorks for Managed Security Services**
- EventTracker for EventTracker Enterprise 7.6
- Trustwave for Trustwave Managed Security Services
- Webroot for Webroot SecureAnywhere Global Site Manager

Reader Trust Award

BEST MOBILE SECURITY SOLUTION

WINNER

AirWatch by VMware for Enterprise Mobility Management

With the growing number of mobile devices used for work, accessing corporate resources on-the-go can introduce a significant threat to enterprise security. AirWatch by VMware Enterprise Mobility Management enables businesses to address challenges associated with mobility by providing a simplified, efficient way to view and manage all enterprise devices. With AirWatch, organizations can manage a diverse fleet of devices. AirWatch ensures mobility deployments are secure and corporate information is protected with end-to-end security for users, devices, applications, content, data, email, networks and more. AirWatch provides real-time device details and continuous compliance monitoring to ensure information is safe. Administrators can access device information, including feature restrictions, compliance status and encryption status within a centralized console. Administrators can maintain advanced encryption on all major devices and platforms, as well as enable containerized encryption for content, applications and email.

AirWatch stands out from its competition because it has the broadest and most flexible mobile ecosystem of any solution on the market. With a fully integrated enterprise mobility management (EMM) suite, including MAM, MDM and MCM, AirWatch offers the most robust feature set to its customers. Cross-platform support is provided for all major mobile and laptop platforms. AirWatch is designed to integrate with most existing corporate infrastructure, streamlining the deployment process and management of devices. AirWatch has also been fully developed internally without relying on third-party solutions. Additionally, AirWatch has built a strong network of NAC vendor partnerships and it has implemented the most OEM APIs of any MDM provider.

Finalists 2015

- **AirWatch by VMware for AirWatch Enterprise Mobility Management**
- Check Point Software Technologies for Check Point Capsule
- Dell for Dell Secure Mobile Access (SMA)
- MobileIron for MobileIron
- Sophos for Sophos Mobile Control

Reader Trust Award

BEST MULTIFACTOR SOLUTION

WINNER

RSA, the security division of EMC, for RSA SecurID

In the data security industry today, the market needs are constantly evolving in response to the changes in technology and also to the IT threat landscape. With the increasing number of data breaches, expanding threat surfaces and an expanding number of devices and users that are accessing data, it is a crucial time for organizations to ensure they are properly protecting users – beginning with identity and access management.

The RSA SecurID solution protects user identities, 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. The RSA SecurID product supports traditional use cases – such as securing VPN access and network operating systems – and also extends to BYOD, cloud and mobile security use cases that are increasing in popularity within the enterprise.

The RSA SecurID product is a de facto standard for authentication solutions. It has more than 55 million users and is present in 95 of the top 100 Fortune companies.

What sets RSA apart is both the quality of the product and the flexibility of choice. Offering a wide range of authenticator options, including hardware and software tokens, on-demand (SMS) and risk-based (risk score determined by user behavior), the SecurID solution is designed to meet any business use case. Additionally, unlike many competitors which use event-based tokens, RSA authenticators leverage the AES-128 algorithm and are time synchronous – they rely on a time window that closes after 60 seconds, minimizing risk. Finally, RSA offers 400+ fully supported technology integrations with a wide range of applications. RSA SecurID technology integrations are jointly tested by both organizations and documented to ensure a positive customer experience.

Finalists 2015

- CA Technologies for CA Advanced Authentication
- Duo Security for Duo Security Cloud-based Two Factor Authentication
- Entrust for Entrust IdentityGuard
- **RSA, the security division of EMC, for RSA SecurID**
- SecureAuth for SecureAuth IdP

Reader Trust Award

BEST NAC SOLUTION

WINNER

ForeScout for CounterACT

ForeScout CounterACT is a recognized market innovator and leader providing comprehensive visibility into devices, users and applications accessing networks in real-time. CounterACT assesses each device to determine whether it contains any vulnerabilities (OS, anti-virus, application, etc.) or configuration issues. Based on policies that users configure, CounterACT will block, allow or limit network access. Unlike traditional NAC products, which can be too restrictive and disruptive, CounterACT offers the flexibility to configure network access policies that are right for the business, accommodating BYOD, etc.

CounterACT automatically finds and fixes endpoint security problems, saving time and improving the end-user experience. CounterACT can automatically update anti-virus, install agents, trigger an operating system patch, or kill a process or application.

CounterACT works with existing network infrastructures, is non-disruptive and does not require 802.1X configurations. CounterACT works with all leading vendors' switches, wireless controllers, VPN equipment and other infrastructure.

Too, it works without an agent. CounterACT can assess the security status of Windows, Mac and Linux systems without the need to deploy another agent on the endpoints. It interoperates with a wide variety of existing security systems, such as vulnerability assessment, APT detection, SIEM, MDM, VPN, next generation firewalls, etc. By sharing security information and automating security controls, CounterACT saves time, reduces risk exposure and improves ROI from existing purchases. It provides more information about what is on a network, including information about vulnerable applications and processes.

Finalists 2015

- Cisco for Cisco Identity Services Engine
- Cryptzone for AppGate
- **ForeScout for CounterACT**
- Hexis Cyber Solutions for NetBeat NAC
- Trustwave for Trustwave NAC

Reader Trust Award

BEST RISK/POLICY MANAGEMENT SOLUTION

WINNER

SolarWinds for SolarWinds Network Configuration Manager

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

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

Finalists 2015

- Qualys for Qualys Policy Compliance (PC)
- RSA, the security division of EMC, for RSA Archer Policy and Risk Management
- **SolarWinds for SolarWinds Network Configuration Manager**
- Tripwire for Tripwire Enterprise
- Trustwave for Trustwave TrustKeeper Compliance Manager

Reader Trust Award

BEST SIEM SOLUTION

WINNER

LogRhythm for LogRhythm Security Intelligence Platform

LogRhythm's Security Intelligence Platform empowers global organizations to detect breaches and the most sophisticated cyberthreats of today, faster and with greater accuracy than ever before. It meets a critical market need for visibility into threats as an unprecedented number of organizations experience damaging data breaches. Organizations understand that it's no longer a matter of if they'll be breached, but rather when, and LogRhythm provides deep visibility into threats and risks to which they'd otherwise be blind. It works by establishing a baseline of normal network activity in order to accurately detect abnormal activity. LogRhythm identifies early indicators of compromise, enabling rapid response and mitigation. It also helps organizations meet compliance requirements and proactively respond to operational challenges, such a network issues.

LogRhythm uniquely combines enterprise-class SIEM, log management, file integrity monitoring and machine analytics with host and network forensics in a unified security analytics platform. The cornerstone of LogRhythm's Security Intelligence Platform is an award-winning, next-generation SIEM and log management solution. LogRhythm collects and analyzes data from more sources and provides greater out-of-the-box analytics and embedded expertise, delivering broader protection, deeper visibility and more actionable insight than any other solution on the market.

LogRhythm's patented machine analytics are powered by the AI Engine, delivering highly automated and easily customized advanced behavioral and statistical analysis. The AI Engine analyzes all data in real-time and identifies the highest priority security events and compliance violations and delivers a much greater level of accuracy for operations, security and compliance assurance.

Finalists 2015

- AlienVault for AlienVault's Unified Security Management (USM)
- Intel Security for McAfee Enterprise Security Manager
- **LogRhythm for LogRhythm Security Intelligence Platform**
- SolarWinds for SolarWinds Log & Event Manager
- Splunk for Splunk Enterprise

Reader Trust Award

BEST UTM SECURITY SOLUTION

WINNER

Barracuda for Barracuda Firewall

Barracuda Firewall is the next-generation firewall for small to midsized organizations. Barracuda Firewall enables enforcement of granular content and access policies based on Layer 7 application visibility and user-identity awareness, with capabilities that are easy and intuitive to manage. Barracuda Firewall overcomes the security compromises in host- or port-based firewalls, as well as the performance limitations of unified threat management (UTM) appliances, through intelligent integration of on-premise and cloud-based technologies. The powerful on-premises appliance is optimized for high bandwidth sensitive tasks, like packet forwarding and routing, intrusion prevention (IPS), DNS/DHCP services and site-to-site connectivity, as well as CPU intensive tasks, like virus scanning, content filtering and usage reporting.

Barracuda understands how cloud-hosted applications and resources have become integral elements of business operations. All Barracuda Firewalls can be managed from the cloud via the Barracuda Cloud Control portal, without creating separate VPN tunnels to remotely administer firewalls. Barracuda Firewall can leverage the cloud for more compute-intensive content security functions, and avoids continual hardware replacement. Users of Barracuda Firewall can aggregate multiple uplinks to improve business continuity with more reliable connections to cloud services and applications.

Having granular policies for both applications and users enables organizations to regulate applications across user groups. This provides bandwidth control and non-business critical activities. Moreover, by setting policies for specific time intervals and access, bandwidth limits can be applied to business-critical time periods. Further, a comprehensive library of applications is predefined on each Barracuda Firewall.

Finalists 2015

- **Barracuda for Barracuda Firewall**
- Check Point Software Technologies for Check Point 600 Appliance
- Dell for Dell SonicWALL Unified Threat Management
- Fortinet for FortiGate/FortiWiFi-60D-POE
- Juniper Networks for SRX Series Services Gateways

Reader Trust Award

BEST VULNERABILITY MANAGEMENT SOLUTION

WINNER

Rapid7 for Nexpose Ultimate

Rapid7 Nexpose Ultimate provides enterprises the visibility to simplify vulnerability management. By combining critical security controls testing, asset discovery, vulnerability assessment and prioritization with closed-loop vulnerability validation, Nexpose Ultimate enables security workflows focused on fixing the most relevant risks.

Security teams receive a comprehensive and prioritized list of misconfigurations, vulnerabilities and remediation steps for on-premise, cloud and mobile assets along with critical security controls grades (patent-pending algorithm) for desktops and servers. The seamless integration with Metasploit, the premier penetration testing tool, provides vulnerability validation by highlighting which vulnerabilities are exploitable.

Enterprises need the ability to prioritize which assets are most valuable to the business. Nexpose helps organization to address the most significant vulnerabilities, first with RealContext – which highlights assets vital to the business – and RealRisk which provides granular risk scoring based on threat intelligence, such as malware and exploit exposure, CVSSv2 and temporal risk metrics.

Nexpose Ultimate is the only vulnerability management solution aligning offensive technologies with defensive capabilities in a single package. Nexpose Ultimate differs from alternative vulnerability management solutions in several key ways. First, it is the only tool to offer integrated closed-loop vulnerability validation within the solution to let security teams prove vulnerabilities are exploitable. It also returns vulnerability information and compliance data in a single scan. This allows security teams to choose controls to modify the security posture of the entire network or address individual vulnerabilities in order to decrease their exposure.

Finalists 2015

- BeyondTrust for Retina CS Enterprise Vulnerability Management
- Malwarebytes for Malwarebytes Anti-Exploit
- Qualys for Qualys Vulnerability Management (VM)
- **Rapid7 for Nexpose Ultimate**
- Tenable Network Security for Nessus Enterprise Cloud

Reader Trust Award

BEST WEB APPLICATION SOLUTION

WINNER

F5 Networks for F5 BIG-IP Application Security Manager (ASM)

F5 BIG-IP Application Security Manager (ASM) is an agile, scalable web application firewall, securing web applications in traditional, virtual and private cloud environments. BIG-IP ASM addresses emerging threats at the application level. It detects and mitigates application attacks, including DoS/DDoS, brute force and more. It delivers comprehensive protection from web security threats, including DDoS and SQL injection attacks, JSON payload vulnerabilities, web scraping, and more. BIG-IP ASM secures data center applications against OWASP Top 10 threats and zero-days attacks. With leading Layer 7 DDoS defenses, programmability and granular attack visibility, it identifies sophisticated cyberthreats and stops attacks before reaching servers. It offers unsurpassed protection against automated attacks and detailed visibility into violations, attack intensity, impact on servers and grade of mitigation success and correlates multiple violations to identify more sophisticated attacks.

ASM is a scalable, agile WAF, delivering unmatched performance and protection. It offers unparalleled protection against automated attacks with proactive bot defenses distinguishing non-human traffic before it reaches servers and commences attack. Its proactive defense combined with reactive automated attack defenses provides comprehensive protection against unauthorized bot traffic. ASM also leads in DAST integration, automatically notifying DAST services when app changes occur, accelerating testing and virtual patching and sealing vulnerabilities immediately. ASM also provides protection most out-of-band solutions cannot – ASM accurately profiles browsers, defends against bots, protects against CSRF, identifies files containing viruses and mitigates Layer 7 DoS attacks.

Finalists 2015

- Alert Logic for Web Security Manager
- Barracuda for Barracuda Web Application Firewall
- **F5 Networks for F5 BIG-IP Application Security Manager (ASM)**
- Fortinet for FortiWeb-1000D Web Application Firewall
- Trustwave for Trustwave Web Application Firewall

Reader Trust Award

BEST WEB CONTENT MANAGEMENT SOLUTION

WINNER

Websense for Websense TRITON AP-WEB

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

Websense TRITON AP-WEB uses TruHybrid technology to combine on-site appliance and cloud security with a unified console to offer complete protection against malware and data theft for employees in all locations. It also offers TruWeb DLP for data theft and loss protection. Its advanced classification engine (ACE) provides real-time security and data analysis to safeguard organizations from evolving web threats.

Websense analyzes and categorizes dynamic web content/threats in real-time, at point-of-click, to detect advanced payloads, exploited documents, mobile malware and much more. Between 3-5 billion requests per day from 900 million endpoints are inspected. Several independent Miercom tests recognized its ability to protect against more advanced malicious scripts and zero-days than any other content management solution. No other solution accurately classifies and analyzes HTTPS and social sites for threats, active scripts and malicious code. It extends hundreds of use policies for social websites that old-school URL filtering cannot accurately classify. Embedded TruWeb DLP enables safe outbound communications, preventing data disclosure even through scanned images, drip DLP and criminally-encrypted control communications.

Finalists 2015

- Blue Coat Systems for Blue Coat PacketShaper
- Cisco for Cisco Web Security Appliance
- EdgeWave for iPrism Web Security
- iboss Network Security for iboss Secure Web Gateway
- McAfee for McAfee Web Protection
- **Websense for Websense TRITON AP-WEB**

Excellence Award

BEST CUSTOMER SERVICE

WINNER

Proofpoint.com for Proofpoint Customer Support

Proofpoint delivers true, 24/7/365 customer support online and from multiple support centers around the world. The Proofpoint support website provides customers with complimentary access to a comprehensive set of online services, including installation documentation, downloadable online manuals, user-oriented manuals and a knowledge base featuring thousands of searchable articles. Customers can also submit tickets, track cases, access training and become a Proofpoint Accredited Engineer through a three-to-five hour self-paced course.

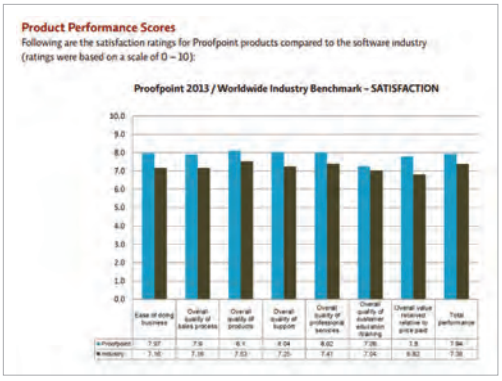
Proofpoint customer support documentation has a proven track record of success. Proofpoint actively monitors documents that are being accessed and has consistently seen a positive response. Proofpoint prides itself on effective customer service and support. Because it stands by its solutions, every Proofpoint hosted-services customer receives Platinum Support. This program provides phone access to technical support engineers 24/7 for high priority issues, as well as 24/7 access to the online Proofpoint Enterprise Support Portal. Customers can submit an unlimited number of cases and access tech documentation.

Results show that 85 percent of Proofpoint support cases are successfully closed by first level support engineers. This excellent track record speaks to the commitment and dedication of the Proofpoint team to clearly address questions in a timely, effective manner.

Proofpoint provides complimentary 24/7 telephone support for priority issues with its technical support engineers to all customers. Proofpoint offers customers web-based downloads from the online knowledge base at no additional charge. Proofpoint's knowledge base has content spanning the previous eight years and is consistently updated.

Finalists 2015

- Barracuda
- **Proofpoint**
- Qualys
- Rapid7
- Thycotic



Excellence Award

BEST EMERGING TECHNOLOGY

WINNER

Cylance for CylancePROTECT

Cylance addresses the needs of the endpoint protection market. Cylance detects and protects against all types of threats (advanced persistent threats, malware, PUPs, adware, etc). In the current environment of targeted attacks by state actors and malware development networks, Cylance raises for the attackers the amount of effort required to evade defenses. Most existing technologies have fundamental flaws that are easy for hackers to overcome, as is evident by the volume of breaches.

Cylance seeks to change the landscape by using machine-learning technology to protect and block threats that no one has seen before. Cylance believes that protection should not be reactive, but should raise the barrier to entry with machine-learning technology that has the ability to adapt and learn.

Today's attackers are using more sophisticated methods of evasion to bypass organizations' security systems. Cylance technology is able to detect previously unknown malware by comparing the malware's DNA against those of tens of millions of existing malware. The product also has features to integrate into other products, like SIEMs and network appliances.

Cylance introduced its products, CylancePROTECT and CylanceV, in early 2014 and has gained more than 100 customers in its two full quarters of product bookings. Its quarter-over-quarter growth this fiscal year is at 140 percent. Expected growth over the next year is over 500 percent.

Cylance has in-house service and support teams which provide assistance with deployment of its products and consulting services 24/7/365. Many customers choose to outsource the management of their security analysis and threat analysis to Cylance.

Finalists 2015

- Cisco for Cisco Advanced Malware Protection
- **Cylance for CylancePROTECT**
- Proofpoint for Proofpoint Threat Response
- Palo Alto Networks for Traps Advanced Endpoint Protection
- Skyhigh Networks for Skyhigh Secure

Excellence Award

BEST ENTERPRISE SECURITY SOLUTION

WINNER

Cisco for Cisco FirePOWER

Cisco FirePOWER solutions are deployed in nearly all countries worldwide and within large portions of the Fortune 100, Global 500 and across all U.S. military branches and in large civilian government agencies.

Sourcefire was acquired by Cisco in November 2013, and the number of customers is growing and pipelines have increased significantly. In addition, the number of partner/resellers has expanded.

Cisco recently introduced Cisco ASA with FirePOWER Services – the industry's first, threat-focused next-generation firewall (NGFW) which delivers superior, multi-layered protection, improves visibility and reduces security costs and complexity. This solution combines Cisco's industry-leading ASA firewall with Sourcefire's industry leading next-generation IPS (NGIPS) and advanced malware protection (AMP) in a single device.

Third-party validation for industry-leading security effectiveness, low TCO, performance, execution and vision also fuels growth.

Cisco's flexible service/support model includes a newly created global security sales organization consisting of 5,000-plus security experts; SMARTnet 24/7 support, hardware repair/advanced replacement and ongoing product updates; education and certifications on FirePOWER solutions via classroom, on-site and computer-based training; extensive professional services offerings; support via 750-plus certified reseller and distribution partners; real-time threat intelligence working around the clock to protect customers – Cisco Talos discovers, assesses and responds to the latest attacks and vulnerabilities; Cisco's Collective Security Intelligence Cloud, fueled by users who share the latest threat intelligence; and the snort.org community, which provides ongoing security enhancements and testing.

Finalists 2015

- **Cisco for Cisco FirePOWER**
- CyberArk for CyberArk Privileged Account Security Solution
- Palo Alto Networks for Palo Alto Networks Enterprise Security Platform
- Splunk for Splunk Enterprise
- Vormetric for Vormetric Data Security Platform

Excellence Award

BEST REGULATORY COMPLIANCE SOLUTION

WINNER

Qualys for Qualys Policy Compliance

Qualys Policy Compliance (PC) is a cloud service that performs automated security configuration assessments on IT systems throughout the network. It helps organizations to reduce risk and continuously comply with internal policies and external regulations. Built on a leading cloud security platform, Qualys PC frees organizations from the substantial cost, resource and deployment issues associated with traditional software products without the use of software agents. Known for its fast deployment, ease of use, unparalleled scalability and integration with enterprise GRC systems, Qualys PC enables IT teams to see how controls relate to critical frameworks and regulations, including CIS, COBIT, ISO 17799 & 27001, NIST SP800-53, ITIL v2, HIPAA, FFIEC and NERC-CIP.

The Qualys PC portfolio includes Qualys Questionnaire, a cloud service that helps centralize and automate the gathering of risk data and compliance evidence from employees, partners, vendors and other subject matter experts, to manage assessment programs efficiently and reliably online.

Qualys Policy Compliance is available as part of the Qualys Security and Compliance Suite. Qualys Policy Compliance annual subscriptions are sold on a per IP basis and include an unlimited number of compliance audits and Qualys' standard 24/7/365 support and updates.

Qualys Policy Compliance provides a fully automated way to satisfy requirements of policy compliance sans agent, fulfilling the policy and compliance industry's need for a low cost, flexible solution. Included in this offering is the collection of OS, application and database configuration access controls from the information assets within the enterprise.

Qualys PC is CIS-certified and provides an extensive library of more than 15,000 checks, spanning more than 50 technologies.

Finalists 2015

- Agiliance for RiskVision 7
- **Qualys for Qualys Policy Compliance (PC)**
- Tenable Network Security for SecurityCenter Continuous View
- Tripwire for Tripwire Enterprise
- Trustwave for Trustwave TrustKeeper for Compliance

Excellence Award

BEST SECURITY COMPANY

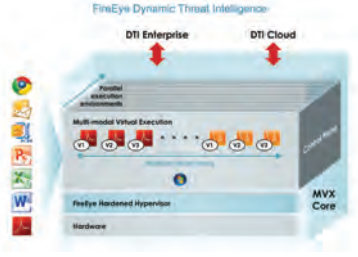
WINNER

FireEye

FireEye continues to grow its customer base and revenues at a 50 percent clip. Today, it has more than 2,000 customers, including many Fortune 1000. Its product line is comprehensive. It helps enterprises deploy effective security programs to incorporate strategies that reduce their target surface and shorten the "alert to fix" cycle to diminish the impact of any security breaches that do occur. Effective security-conscious organizations can, with FireEye, gain the following: strong preventive measures to minimize attack surface area; advanced detection capabilities (signature-less and real-time detection); network, endpoint and event visibility; the threat intelligence required to leverage the visibility; a fluid process to adapt to emerging threats; and forensics for both network and endpoint insight.

As attacks change, defensive measures must evolve. FireEye has learned the next-generation security architecture needs to be adaptive, nimble and have real long-term relevance. And it approaches this with state-of-the-art products, highly skilled security experts and real-time threat intelligence.

All customers get email, live chat, web and telephone support 24/7/365 for up to 15 designated callers, with a one-minute target response time and immediate escalation to level three advanced support engineering for highest severity issues with 30-minute response times. FireEye's platinum priority plus program adds immediate problem escalation to level three advanced support engineering; an unlimited number of designated callers, with secure support website/portal access for those callers; a designated support engineer (DSE) assigned to clients. FireEye also provides an annual on-site review of service and product performance and on-site technical assistance, monthly support statistic reporting, and a quarterly business review via conference call.



Finalists 2015

- Check Point Software Technologies
- **FireEye**
- Qualys
- Trend Micro
- Veracode

Excellence Award

BEST SME SECURITY SOLUTION

WINNER

Check Point Software Technologies for Check Point 600 Appliance

Check Point is a worldwide leader in securing the internet, serving more than 100,000 customers, including 100 percent of the Fortune 100 and 97 percent of the Fortune 500. Achieving these customer results was possible because Check Point seeks to provide enterprise-level technologies to all companies, regardless of size. Security gateway appliances, such as the 600 Appliances, are crucial security technologies for companies, and therefore, it is clear that security gateways have a customer base of thousands of enterprise customers worldwide. The 600 Appliances, for example, have received remarkable reviews from customers and analysts since the product launch in May 2013.

World-class 24/7 support is available for all products and services. "Purchase support," which can be found on the website, enables customers to have a purchase quote if he/she is aware of the right enterprise solution. The "compare support" option details the levels of service that Check Point provides. These levels include standard, premium, elite and diamond (an addition to premium or elite). There is a "standard support" option which provides phone number information for different Check Point regions. Service is available through the phone line 24/7.

And lastly, a security expert newsletter is published, which provides further beneficial information for companies seeking tech tips, information on the latest software releases, and training and certification updates. Professional Services offer a comprehensive range of services to help companies protect and extend their security investment, including design services, implementations and upgrades, custom training, technical account management and network optimization services.

Finalists 2015

- Barracuda for Barracuda Spam Firewall
- **Check Point Software Technologies for Check Point 600 Appliance**
- iSheriff for iSheriff Cloud Security
- Network Box USA for Network Box Managed Security Solution
- Qualys for Qualys Express Lite

Excellence Award

ROOKIE SECURITY COMPANY OF THE YEAR

WINNER

Cyphort

Cyphort exited stealth in February 2014 and has seen tremendous quarter-over-quarter growth, beating expectations each quarter. Since February, the company has grown 125 percent in company size, has won numerous awards and accolades from several publication and was shortlisted as one of the 10 most innovative companies at RSA 2014. Recently, Dell named Cyphort to this year's class of Founders 50 innovators. Cyphort customers, such as Netflix, praise Cyphort in press releases and on social media on a regular basis. Cyphort's outlook for 2015 points to an even stronger trajectory.

Cyphort is one of the only software-based advanced malware protection solutions on the market that has instant scalability capabilities, can be deployed as an appliance, as software on common hardware, or in a virtualized infeastructure with support for detection Windows and Mac OSX threats across web and email in one solution. Cyphort's platform was developed by Ali Golshan, a former CIA/NSA threat researcher, data scientist and serial product entrepreneur, and Fengmin Gong, who co-founded Intruvert and Palo Alto Networks, as well as serving as the chief architect/threat research leader of FireEye. Cyphort's flexible, API-driven architecture lends itself to be applied in a wide variety of models, be it cloud, software-defined or "traditional" networking. Its API-based architecture allows for bi-directional integration with endpoint-based APT protection solutions, offering customers more in depth and informative threat assessments, and with existing security controls, demonstrating its ability to automate detection and response.

Cyphort is committed to providing customers with an excellent experience and ensuring their long-term success with its products.

Finalists 2015

- **Cyphort**
- Elastica
- Netskope
- Skyfence
- Sumo Logic

Professional Award

BEST CYBERSECURITY HIGHER EDUCATION PROGRAM

WINNER

Champlain College for Cybersecurity and Digital Forensics

The students at Champlain College dive right into forensics and security courses their first semester, they do not have to wait until their junior year as at many other colleges. Students have access to an education other colleges cannot provide, with more than 35 industry-specific courses in on-campus, online and graduate programs – all developed and taught by experts in the field. Students use the tools and procedures currently being used in the field. They conduct forensic research and produce case studies on the latest technologies, which have included Amazon Kindle and Google Glass. This year they will be working on the latest wearable technologies and health applications on mobile devices. These case studies are published on computerforensicsblog.champlain.edu and some will be presented at national conferences, such as CEIC. This year students collaborated on an award-winning app to assist law enforcement in conducting digital forensics work faster than ever.

Champlain conducts an "Imagine College" program for underserved students. These students are able to explore college as an opportunity they thought was out of reach, highlighting the career growth and opportunities this emerging field offers. Champlain also hosts an annual event for seventh and eighth graders featuring digital forensics and cybersecurity as career options. Another innovative draw to students interested in this profession is the opportunity to work in Champlain's Leahy Center for Digital Investigation, a custom-designed, enterprise-level forensics laboratory. The lab is capable of employing up to 60 students to work on real forensics cases for private businesses and law enforcement entities under the supervision of faculty, lab staff and Director Jonathan Rajewski.

Finalists 2015

- **Champlain College for Cybersecurity and Digital Forensics**
- **(ISC)² for Global Academic Program**
- **SANS Technology Institute for Master of Science in Information Security Engineering**

Professional Award

BEST PROFESSIONAL CERTIFICATION PROGRAM

WINNER

(ISC)² for CISSP

In a world fraught with security threats and breaches, the need for skilled and knowledgeable information security professionals has never been greater. With more than 25 years in the industry, (ISC)² offers IT security professionals worldwide access to unparalleled education opportunities that facilitate deeper knowledge and stronger skill sets, along with valuable peer networking and mentoring. Considered the gold standard of IT security credentials, the CISSP is a measure of excellence held by nearly 100,000 CISSPs in 139 countries. As the globally recognized standard of competence, the CISSP Common Body of Knowledge (CBK) is the best reference available and reflects up-to-date, relevant topics in the ever-changing field of information security. Some of the most highly respected, high-profile IT security luminaries around the world hold the CISSP. With the advances in technology and the evolving threat landscape, the CISSP represents core IT security concepts that professionals need to thrive in the industry today.

Frequently referenced in top lists of IT-related certifications, the CISSP is known as the benchmark of professionalism. Required by some of the world's most security-conscious organizations and government entities, the CISSP validates that information security leaders possess the breadth of knowledge, skills and experience required to credibly build and manage the security posture of their organizations. This breadth of knowledge and the experience it takes to pass the exam are what set the CISSP apart. An analysis by Burning Glass Technologies stated that 56 percent of cyber jobs in the contracting industry require the CISSP. The CISSP is an IT security certification of firsts – first to meet ANSI/ISO/IEC requirements, first to require high-quality, auditable continuing professional education credits, and one of the firsts to be listed as a job requirement in the U.S. DoD 8570.1 matrix.

Finalists 2015

- **(ISC)² for Certified Secure Software Lifecycle Professional (CSSLP)**
- **(ISC)² for CISSP**
- **Global Information Assurance Certification (GIAC) for GIAC Security Expert (GSE)**
- **ISACA for Certified information Security Manager (CISM)**
- **ISACA for Certified Information Systems Auditor (CISA)**

Professional Award

BEST IT SECURITY-RELATED TRAINING PROGRAM

WINNER

Guidance Software for EnCase

Through September 2014, Guidance Software's 100-plus instructors have trained more than 64,000 students worldwide, communicating the breadth and depth of the digital investigations training. As the volume and complexity of cyberthreats continue to increase, IT security professionals, corporate and law enforcement investigators can use EnCase tools to collect in a forensically sound way, analyze and take action on static and volatile digital evidence. By taking advantage of Guidance Software's training, digital investigators are ensured that their skills are best tuned to uncover new and advanced threats in enterprise investigations, data audits or computer security incident response tasks. From courses designed by professionals for professionals just beginning their careers in computer forensics to classes focused on helping investigative experts to gain specialized skills in cybersecurity, incident response or eDiscovery, Guidance Software's training program sets the standard in digital investigation instruction.

Guidance Software is meeting the needs of IT security professionals, corporate users and law enforcement investigators by offering a variety of training career tracks and new training courses focused on today's security challenges. In addition to its state-of-the art training facilities and authorized training partners around the globe, Guidance Software can bring its training courses to customers through its EnCase Mobile Training program or its OnDemand and OnLive options. In addition, the company is continuously updating course offerings, including its EnCase CyberSecurity and Analytics, EnCase Macintosh Examinations and EnCase Host Intrusion Detection courses. More than 6,000 professionals will be armed that way year over year with the needed training to evolve with the fast-changing security landscape.

Professional Award

BEST SECURITY TEAM

WINNER

Troy University IT Secure Operations Team for Troy IT SOC

The Troy IT SOC is a cross-division, multi-disciplinary team. Representatives from the business and academic units work alongside the IT team to manage information security strategies. Executive sponsorship at the highest level has been pivotal to the success of the team – the executive management team participates in quarterly security operations updates and active pursuits of enhanced security technologies. Through these collaborative efforts, security governance and execution facilitate institutional awareness of all aspects of the secured operations program. Using third-party consultants, the team is exposed to independent reviews and given guidance on operational activities. The team is led by the CSO and co-chaired by rotating members appointed by the faculty senate and administrative services unit.

Awareness and inclusion are the major contributors to gaining support with the executive team and constituents throughout the institution. Troy IT SOC operates a number of information distribution mechanisms. Its website presents current and archived information, and it employs Twitter and SMS subscription tools to distribute any emergency notifications.

Additionally, it produces a quarterly security awareness bulletin and subscribes to the SANS Securing the Human project. As well, it briefs the senior executive every quarter on all data security operations. Through inclusion of all major stakeholders and data managers, Troy IT SOC fosters collective appreciation for security best practices. Further, as part of new employee orientation, all candidates participate in security awareness training. This training is role-specific, requiring annual review and the passing of a proficiency exam.

Finalists 2015

- (ISC)² for (ISC)² Education/Training Program
- **Guidance Software for EnCase**
- RSA, the security division of EMC, for RSA Education Services' Advanced Cyber Defense Curriculum
- SANS Institute for SANS Securing the Human (STH)
- Wombat Security Technologies for Security Education Platform

Finalists 2015

- Government of New Brunswick for Security Event Management Team
- **Troy University IT Secure Operations Team for Troy IT SOC**
- Voya Financial for Technology Risk and Security

Professional Award

CSO OF THE YEAR

WINNER

Christopher Ipsen, CISO, state of Nevada

In his seven years as CISO of the state of Nevada, Chris Ipsen has used a multifaceted approach to address the difficult challenge of workforce within a state government – where pay is lower and responsibility is high. With clear objectives mapped to national strategies and focusing on the long-term needs of the state, he incrementally selected a diverse core security group from varied technical backgrounds: WAN, Unix, Windows, programming, database, mainframe and compliance. Individuals were then assigned primary security roles in their areas of expertise and secondary roles as backups. Primaries were assigned the responsibility of establishing standards and procedures in their areas and to train secondary personnel. The teams were then assigned responsibility to present and train agency ISOs at monthly state IT security meetings. Teams review and contribute to standards collaboratively. The net result is a sustainable, multifaceted group – diverse by gender and capability – with a low turnover and high motivation.

Christopher Ipsen has earned the support of senior leadership within the state and with corporate partners by having a well-defined plan focused on business solutions rather than technical problems. In developing solutions, he works with technical resources to understand the problem to be solved and the possible solutions. He then works diligently to negotiate the correct solution to achieve the most efficient enterprise outcome based on technology, context, opportunity, human resources, risk and cost. Although he has a high technical competence and is active with key standards bodies like NIST, he carefully avoids tech speak when dealing with business leaders. With a pleasant, passionate and calm demeanor, he assists leaders to understand the business decisions needed for effective risk avoidance.

Finalists 2015

- Gene Fredriksen, CISO, PSCU (Public Service Credit Union)
- **Christopher Ipsen, CISO, state of Nevada**
- John Masserini, CISO, MIAX Options
- Myrna Soto, CISO, Comcast
- Bruce Wignall, CISO, Teleperformance Group

Professional Award

EDITOR'S CHOICE

WINNER

Online Trust Alliance

The stated mission of the Online Trust Alliance (OTA) is to enhance the integrity of transactions occuring on the web. Under the indefatigable leadership of Craig Spiezle, executive director, founder and president, its efforts over the past decade have helped enhance data protection for countless businesses, as well as bolstered the privacy of individuals.

The information it provides to a broad range of stakeholders – ranging from business and technical decision-makers and privacy and security professionals to web and app developers – increases understanding of the issues and solutions that can not only improve data protection practices, but in the almost certainty of a breach, aid them in developing and implementing business readiness plans.

Earlier this year, with the release of guides for data protection and risk assessment, it once again demonstrated its advocacy for best practices to help organizations in both the public and private sector.

And, just this past March, the OTA wrote a letter to Congress – in response to President Obama's proposed *Personal Data Notification & Protection Act* – listing points it believes are imperative to creating a complete federal data breach notification law. Notably, the nonprofit says a federal law needs to preempt the existing 47 state laws and must also contain a safe harbor from regulator penalties for businesses or organizations that demonstrate a commitment to the adoption of best security and privacy practices. The group also wrote that any law should "contain an appropriate coverage of personal information triggering notification obligations."

"As an individual's online worlds grows and expands...so must the protections afforded to them," the group wrote.

We're delighted to honor the OTA's efforts.

Online Trust Alliance team: Craig Spiezle, executive director; Scott Stein, VP, public policy; and Liz Shambaugh, director of member services.

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