AWARDS 2010

Honored in the U.S.

March 2, 2010 • San Francisco

SC AWARDS 2010
MAGAZINE Honored in the U.S.

Contents

Meeting challenges

Companies move swiftly to take advantage of new technologies to get an edge on the competition. Often, this leads to security vulnerabilities too big to ignore. A host of data breaches have occurred at tons of companies over the past year to prove this.

But, a change is occurring. Information security is getting much more attention from many corporate executives than in the past. They are beginning to understand the risks poor information security planning can cause. More importantly, C-level executives are entrusting their information security leaders to make information security a fundamental part of overall business operations. The likes of cloud computing platforms and services, virtualized environments, Web 2.0 applications and more are becoming an integral part of critical business initiatives. At the same time, concerns about safeguarding the data shared through these means are leading to the development of extensive security policies and the deployment of technologies and rules to ensure these are followed. And, while the poor economic climate that impacted us all last year is beginning to show some signs of recovery, the many trials associated with emaciated budgets have seen information security professionals rise to still other challenges.

The SC Awards program celebrates this unyielding, determined spirit. This year, finalists were chosen from more than 600 entries for the Reader Trust, Excellence and Professional Awards categories. These are judged by panels of leading security officers from all major vertical markets. The Reader Trust Awards panel was created through invitation of more than 1,000 end-users of security technology. And, the more than 25 Excellence and Professional Awards judges were selected by us for their industry expertise. The panels conduct in-depth analysis and consider many factors in narrowing down the field to reach our list of finalists and, ultimately, our winners. These companies and professionals represent the best of the security industry. They are just some of this vibrant marketplace's leading lights and we're excited to extol their skills, innovation and accomplishments during yet another SC Awards.

– Illena Armstrong, editor-in-chief, SC Magazine

EDITORIAL
EDITOR-IN-CHIEF Illena Armstrong

2010 SC AWARDS U.S.
SENIOR EVENTS MANAGER Pilar Mustafa
EVENTS MANAGER Natasha Mulla
EVENTS MANAGER Shital Patel
EVENTS ASSISTANT Ashley Hewlett

DESIGN AND PRODUCTION
GROUP DESIGN DIRECTOR Sandra DiPasqua
ART DIRECTOR Brian Jackson
MANAGING EDITOR Greg Masters
GROUP PRODUCTION MANAGER, MARKETING DIVISION Shannan Miller
VP OF PRODUCTION Louise Morrin
SENIOR PRODUCTION CONTROLLER Krassi Varbanov

U.S. SALES
ASSOCIATE PUBLISHER, VP OF SALES Gill Torren (646) 638-6008
EASTERN REGION SALES MANAGER Mike Shemesh (646) 638-6016
WESTERN REGION SALES MANAGER Matthew Allington (415) 346-6460
NATIONAL INSIDE SALES EXECUTIVE Brittany Thompson (646) 638-6152
NATIONAL ACCOUNT MANAGER - EVENT SALES Mike Alessie (646) 638-6002
SALES/EDITORIAL COORDINATOR Katy Wong (646) 638-6104
GROUP CIRCULATION MANAGER Sherry Oommen (646) 638-6003

MANAGEMENT
MANAGING DIRECTOR Lisa Kirk
CHAIRMAN William Pecover
DEVELOPMENT DIRECTOR Tony Keefe

Words from the co-chairs

We've known for a very long time now, that the "fortress" approach to information security is ineffective. This year, thanks to a slowly recovering economy, our business requirements are forcing us to find new and innovative approaches to secure and protect our most critical information. Whether driven by M&A, outsourcing or "cloud" computing, organizations are being forced to rethink their strategic approaches to information protection.

As we face more customized and targeted attacks going after intellectual property, or incredibly organized approaches to financial fraud and identity theft, the strategies and technologies we rely on are changing rapidly. We are seeking innovative and increasingly cost-effective ways to bolster our defenses and increase both our preventative and detective capabilities.

The challenge is great. The impressive thing about the information security community is how well they react to challenges. We see CISOs realigning their functions and processes, creating a more reactive security function. We see technology innovators finding innovative solutions to complex problems. We see a community of professionals working together to share leading practices and support each other. This community is always willing to rise to face great challenges.

My predictions for 2010 is that there will be more regulatory challenges. There will be more data losses of personally identifiable information. We will see an increase in targeted attacks and custom malware. Business will become more complex. Budgets will still be tight. And the great CISOs and security community will continue to find new and inventive solutions to these challenges.

I would like to congratulate the nominees and the winners of the 2010 SC Awards U.S.

– Greg Bell, global services leader, information protection and business resiliency, KPMG LLP; co-chair, SC Awards Committee

The first decade of the new millennium has been an amazing journey in the world of information security. In 2000, most of us were breathing a collective sigh of relief that, for the most part, our Y2K fears did not come to fruition, and we could return to our normal day-to-day responsibilities. Who knew then that the information security landscape would change so dramatically? We learned a new term, "personally identifiable information (PII)," and the laws that govern it. It is incredible that it used to be normal operating procedure to have customers include a Social Security number on a check, or that companies wouldn't think twice to use it as a database primary key. Today, PII is treated almost as radioactive material – to be removed where possible, but otherwise protected at great cost to prevent damage to customers and employees.

In addition to the changing threat landscape, there is an alphabet soup of standards and regulations that were created and needed to be addressed depending on industry and business type. Innovative technologies, such as social media, have been game-changers in the way that we interact with each other, and cloud computing is changing the way we do business.

Through it all, the dedication, innovation and creativity of the information security world continues to provide brilliant new ideas to combat threats, foster innovation and make our information safer. I am proud to be a member of this industry and delighted *SC Magazine* highlights these innovations throughout the year and then coordinates an awards ceremony where these talented companies and individuals are rewarded with recognition for their hard work and dedication. This next decade will certainly bring new challenges, and I am confident that the people in our industry will meet them. Congratulations to everyone and thank you for your outstanding efforts.

– Stacey Halota is vice president, information security and privacy at The Washington Post Co. She was SC Magazine*'s CSO of the Year in 2009.*

The Judges

CO-CHAIR
Illena Armstrong is editor-in-chief of *SC Magazine*. She and her team have received nine ASBPE Awards for excellence.

CO-CHAIR
Greg Bell is global services leader, information protection and business resiliency at KPMG LLP.

CO-CHAIR
Stacey Halota is VP, information security and privacy at The Washington Post Co.

Rich Baich is a principal at Deloitte & Touche. He has led teams designing, implementing, measuring and advising organizations.

Jennifer Bayuk is a principal at Jennifer L Bayuk LLC. She is an information risk management consultant.

Dennis Brixius is VP, risk management & CSO at The McGraw-Hill Cos. He was *SC Magazine*'s CSO of the year in 2007.

Rufus Connell is VP, information and communication technology at Frost & Sullivan. He oversees its N. American research business.

Dave Cullinane is CISO & VP at eBay. Formerly, he was CISO for Washington Mutual.

Jerry Dixon is director of analysis for Team Cymru.

Thomas Dunbar is global IT chief security officer at XL Capital. He was *SC Magazine*'s CSO of the year in 2006.

Patricia Edfors is chief privacy and security officer at Mirixa Corp.

Michele Edson is senior vice president - marketing and sales director for The Santa Fe Group.

Gene Fredriksen is the senior director and global information security officer for Tyco International.

André Gold is VP & CISO for MoneyGram Intl. Formerly, he was the VP of security for ING Financial Services.

Maurice Hampton is information security program manager at GE - Global Infrastructure Services.

Steve Katz is president of Security Risk Solutions. He has been called the grandfather of all CISOs for his early work at Citigroup.

Daniel Lohrmann is CTO for the state of Michigan. He was *SC Magazine*'s CSO of the year in 2008.

J. Laz Montano is AVP, enterprise infrastructure IT risk and compliance at MetLife.

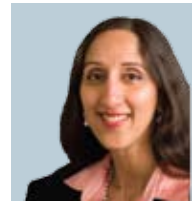
Yonesy Nunez is director, information security at The New School. He manages internal and external information security issues.

Randolph Sanovic is director, information security at General Motors Corp.

Vito Sardanopoli is manager of information security & compliance at Tiffany & Co.

Stephen Scharf is SVP and global CISO for Experian.

Howard Schmidt is the nation's cybersecurity coordinator, reporting to President Obama.



Simone Seth is a director at Pricewatehouse-Coopers, serving as an industry analyst for the Information Security Forum.

Craig Spiezle is executive director of the Online Trust Alliance. He is responsible for setting the strategic vision of the organization.

Mark Thyer is a security analyst for the California Department of Health Care Services.

Larry Whiteside is CISO of the Visiting Nurse Service of New York.

The Sponsors

SC Magazine would like to thank all of our sponsors for their generous support of the 2010 SC Awards U.S. Their involvement has made this event possible, which helps raise professional standards in the information security industry worldwide.

BeyondTrust

www.beyondtrust.com

BeyondTrust provides privilege authorization solutions for heterogeneous IT environments. The BeyondTrust customer retention rate is over 90%. The company is headquartered in Los Angeles, with East Coast offices in the Boston Area.

eBay

www.ebay.com

With more than 88 million users globally, eBay is the world's largest online marketplace, where practically anyone can buy and sell practically anything. eBay connects a diverse community of buyers and sellers, as well as small businesses.

ESET

www.eset.com

ESET is a leading developer of security software for businesses and consumers, protecting over 90 million systems worldwide. Award-winning ESET NOD32® Antivirus offers superior anti-malware protection.

Modulo

www.modulo.com

Modulo is a global market leader for GRC management. Modulo's recent honors include: Hot Company 2009 and Global Excellence Customer Trust Award 2009, validating Modulo's commitment to its product innovation.

NetWitness

www.netwitness.com

NetWitness provides patented and award-winning, next-generation security solutions that help organizations discover, prioritize and remediate complex IT risks. NetWitness has offices in the U.S. and the U.K. and global partners.

Qualys

www.qualys.com

Qualys is a leading provider of on demand IT security risk and compliance management solutions. Qualys' SaaS solutions are deployed in hours, providing customers a continuous view of their security and compliance postures.

Schwartz Communications

www.schwartz-pr.com

Schwartz Communications has deep experience helping companies achieve their corporate and product marketing goals. Schwartz provides the expertise of a large agency, with the approach of a small firm.

Sentrigo

www.sentrigo.com

Sentrigo is a recognized innovator in database security. The company's Hedgehog software provides full-visibility database activity monitoring and real-time protection to defend mission-critical data against inside and external misuse.

Tenable Network Security

www.tenablesecurity.com

Tenable Network Security provides solutions that unify real-time vulnerability, event and compliance monitoring into a single, role-based interface.

TippingPoint

www.tippingpoint.com

TippingPoint is a global provider of network security solutions that address the needs of complex network environments.

TriGeo Network Security

www.trigeo.com

TriGeo Network Security delivers enterprise security information and event management designed specifically for the mid-market.

BEST ANTI-MALWARE SOLUTION

WINNER

McAfee for McAfee Web Gateway
www.mcafee.com

As use of the web continues to grow and evolve, web-borne malware attacks continue to grow and evolve as well. McAfee Web Gateway offers powerful, proactive protection against the malicious and targeted attacks that are a predictable part of doing business in a Web 2.0-enabled world. Widely deployed reactive security solutions – such as signature-based anti-virus and category-only URL filtering – are still important for blocking "known bad" behavior and content. But these reactive techniques were never designed to combat today's exploits. For example, they can't prevent attacks that entice users to unwittingly click on a link that downloads a virus designed to evade signature-based detection, or attacks that hide malicious code within seemingly good HTTP or HTTPS traffic. The ability to proactively block unknown – as well as known – threats has become crucial.

McAfee Web Gateway uses next-generation proactive intent analysis to filter out malicious content from web traffic in real time. By scanning a web page's active content, emulating and understanding its behavior and predicting its intent, McAfee Web Gateway proactively protects against zero-day and targeted attacks as they occur. Outbound malware detection identifies and isolates existing infections phoning home, and prevents sensitive data from leaving the organization through Web 2.0 sites. The proactive threat protection against unknown malware is fueled 24/7 by McAfee Global Threat Intelligence, and accompanied by comprehensive, "traditional" anti-virus protection to block known malware. Combining next-generation proactive analysis, outbound malware detection and anti-virus capabilities provides a unique gateway-specific anti-malware technology and strong defense against malware.

Even 'simple' infections can cause an entire IT staff a significant amount of overhead in chasing infected machines, not to mention the data leakage risks and damage to a brand. In one independent test, McAfee Web Gateway (Webwasher) detected 99.9 percent of malicious samples while achieving a .003 percent false positive rate. McAfee Web Gateway offers powerful, proactive protection at the gateway against blended threats, spyware and targeted attacks that are a predictable part of doing business in a Web 2.0-enabled world, eliminating costly cleanup and data leakage.

Finalists 2010

- AVG Technologies for AVG Internet Security Business Edition
- Astaro Internet Security forAstaro Security Gateway
- Cisco Systems for Cisco IronPort S-Series Secure Web Gateway
- ESET for ESET NOD32 Antivirus 4
- McAfee for McAfee Web Gateway
- Symantec for Symantec Endpoint Protection Small Business Edition

BEST COMPUTER FORENSICS SOLUTION

Finalists 2010

- ArcSight for ArcSight Logger
- Guidance Software for EnCase Forensic
- NetWitness for NetWitness NextGen 9.0
- Quest Software for Quest ChangeAuditor
- Solera Networks for Solera DS Network Forensics Appliances

WINNER

Guidance Software for EnCase Forensic
www.guidancesoftware.com

EnCase Forensic is designed for law enforcement and security analysts who need to investigate all types of digital storage devices. It facilitates the search, identification, collection, preservation, analysis and reporting of digital evidence in a court-approved manner. It is the only computer forensic application that has withstood numerous court challenges worldwide.

EnCase has been used in hundreds of thousands of cases worldwide and mentioned in more than 70 published court cases. The EnCase Evidence File, a container for digital evidence that maintains and verifies the chain-of-custody of digital evidence, is a robust evidence container. Tens of thousands of users have worked with EnCase software. Thousands of people have attained EnCase Certified Examiner status. Millions of cases have used EnCase Evidence Files. Nearly every eDiscovery service provider uses EnCase Evidence File. This level of court validation, and the fact that EnCase Evidence Files are a leading preservation/authentication mechanism for digital evidence, makes it the most credible way to collect forensically sound electronic data in the industry today.

EnCase's passive servlet (agent) is simply installed on all machines on the network and awaits instructions. Moreover, it provides a secure way to manage IT/legal personnel's access to network assets. Through the use of Secure Authentication for EnCase (SAFE), users can be restricted from performing search and collect activities in a number of different ways, including by subnetwork, time of day, region, etc. Additionally, all user activity is logged, ensuring compliance with regulatory guidelines.

With EnCase, an enterprise can expect to see a significant reduction in costs associated with electronic data collection. The software's ability to search and collect information over the network in a non-intrusive way allows enterprises to avoid expensive travel costs since it eliminates the need to have personnel travel to remote locations to gather data. Positive customer return on investment (ROI) generally occurs in the short term after implementing EnCase.

Though no analyst firm tracks computer forensic shipments, many professionals in the computer forensics community say Guidance Software is the market leader in this space with more than 33,000 copies of EnCase Forensic sold.

BEST DATA LEAKAGE/EXTRUSION PREVENTION

Finalists 2010

- EMC for RSA DLP Suite
- Fidelis Security Systems for Fidelis XPS
- Symantec for Symantec Data Loss Prevention 9.0
- TippingPoint Technologies for TippingPoint Intrusion Prevention System (IPS)
- Trend Micro for LeakProof

WINNER

TippingPoint Technologies for TippingPoint Intrusion Prevention System
http://tippingpoint.com

The TippingPoint Intrusion Prevention System (IPS) works to monitor outbound traffic and prevent critical data from leaving the corporate network. With the advent of web-based office suites and internet-connected backup technologies, a compromise of a single system can now yield the sensitive data of thousands of organizations, as opposed to just one. Further, organizations are increasingly concerned with customer information being stolen or with intellectual property being leaked to competitors. In all of these situations, data leakage prevention and detection becomes extremely critical. Customers can use IPS filters to identify the packets that would contain that information. If the contents of a particular packet are found to contain sensitive or confidential data, the IPS will then take action based on policies set by the administrator. This can include simply alerting the administrator that this information has gone outbound or it can be blocked leaving from the network altogether.

TippingPoint's network-based, purpose-built hardware solution is flexible enough to be placed at the network perimeter, at remote locations and at the network core. The IPS is transparent in the network and blocks inappropriate traffic in real time, protecting sensitive data from leaving the network, while also supporting compliance regulations. The Digital Vaccine service, the security intelligence in the TippingPoint IPS, offers evergreen security in the form of comprehensive vulnerability filters. These filters are developed to cover the latest threats and can monitor for common data points, such as Social Security numbers, to ensure these don't go out of the network. However, since organizations vary in what they want to protect and how they categorize sensitive data, TippingPoint offers a custom filter service that tailors IPS filters to customers' specific needs. This could include product-naming codes or financial information.

Challenging conditions are placing budget pressures on security executives. At the same time, as today's data center is driving demand for uncompromised security, the organization is driving to reduce IT administrative costs wherever possible. TippingPoint's IPS can be configured to monitor outbound traffic and keep confidential data from being leaked.

BEST ENCRYPTION SOLUTION

Finalists 2010

- BitArmor Systems (part of Trustwave) for Trustwave Data Control
- Check Point Software Technologies for Check Point Full Disk Encryption
- Cisco Systems for Cisco IronPort Email Encryption
- PGP Corp. for PGP Whole Disk Encryption
- Sophos for Sophos SafeGuard Enterprise

PGP®
Whole Disk Encryption

WINNER

PGP Corp. for PGP Whole Disk Encryption
www.pgp.com

Mobile computing has quickly emerged for increasing user productivity. However, the portable nature of these devices increases the possibility for loss or theft. Consequent exposure of sensitive data can result in financial loss, legal ramifications and brand damage. PGP Whole Disk Encryption provides enterprises with comprehensive, nonstop disk encryption for Microsoft and Apple Mac OS X systems, enabling fast, cost-effective protection for data on desktops, laptops and removable media. The encrypted data is continuously safeguarded from unauthorized access, providing strong security for intellectual property, customer and partner data, and corporate brand equity. PGP Whole Disk Encryption protects data without changing the user experience, and automatically enforces data protection with centrally managed policies. Not only is full disk encryption achieved using the existing infrastructure, but operational costs are reduced from centrally automating encryption policies.

In a 2010 encryption tools Group Test in *SC Magazine*, PGP Whole Disk Encryption 9.10 achieved top marks across all testing categories, receiving accolades for the product's easy-to-use nature and extensive documentation. *SC Magazine* stated, "PGP is an industry leader and this product is a great value for the money." As a PGP Encryption Platform-enabled application, PGP Whole Disk Encryption can be used with PGP Universal Server to manage existing policies, users, keys and configurations, expediting deployment and policy enforcement. The tool can also be used in combination with other PGP encryption applications to provide multiple layers of security. PGP Whole Disk Encryption is also available through a managed services provider (MSP) network worldwide. Customers are provided with the same PGP Data Protection with no upfront capital investment and no incremental load on IT resources.

The PGP Encryption Platform enables organizations to address immediate needs and continue to proactively deploy encryption applications without burdening administrators with multiple interfaces or distracting end-users with new training requirements. This approach enables IT to develop a proactive encryption strategy to mitigate risks before they affect operations or threaten the corporate brand and reputation.

BEST ENDPOINT SECURITY SOLUTION

WINNER

Juniper Networks for
Juniper Networks Unified Access Control
www.juniper.net

Juniper's Unified Access Control (UAC) is a standards-based, scalable, comprehensive access control solution that granularly and dynamically controls user access based on identity, device security state and location information. UAC protects networks by guarding critical applications and sensitive data, identity-enables access control and security, and provides comprehensive visibility and monitoring. UAC addresses challenges, such as insider threats, guest access, outsourcing/off-shoring and regulatory compliance.

The tool delivers significant competitive differentiation. UAC provides full Layer 2-7 policy enforcement on a wide array of enforcement points. UAC's policies are enforced at Layer 2 by any vendor's 802.1X-enabled wireless access points or switches, including Juniper Networks' EX Series Ethernet Switches; at Layers 3-7 via any Juniper firewall platform; and full Layer 7 application layer policy enforcement via standalone IDP series appliance. UAC is one of the most scalable NAC solution available.

UAC combines some of the best access control and security technologies while leveraging existing security and network infrastructure investments. User identity, device state and network location is determined by the dynamically deployable, cross-platform UAC Agent or via UAC's agent-less mode, useful where installing a software client is not feasible, such as for guest access. UAC also dynamically delivers role- and resource-based access control of unmanageable devices – such as networked printers, VoIP handsets, health monitoring devices, etc. – making simpler and faster-to-deploy access control across a network regardless of device manageability.

Juniper's Unified Access Control also meets regulatory compliance by ensuring endpoints are assessed pre-/post-admission for security and access policy compliance; applies industry-leading, dynamic anti-spyware/anti-malware protection to endpoints attempting network access; offers secure, encrypted data transport from endpoints into and throughout the network; and correlates user identity and role information to network and application usage, providing significant business and technical advantages for enterprises and SME.

Finalists 2010

- Cisco Systems for Cisco Network Admission Control (Cisco NAC)
- Juniper Networks for Juniper Networks Unified Access Control
- Sophos for Sophos Endpoint Security and Data Protection
- Symantec for Symantec Endpoint Protection 11.0
- Trend Micro for OfficeScan 10

BEST ENTERPRISE FIREWALL

Finalists 2010

- Astaro Internet Security for Astaro Security Gateway
- Check Point Software Technologies for Security Gateway R70
- Fortinet for FortiGate-620B
- Juniper Networks for Juniper Networks SRX Series
- Palo Alto Networks for Palo Alto Networks PA-4000 Series
- SonicWALL for SonicWALL NSA E7500

WINNER

Check Point Software Technologies for Check Point Security Gateway R70
www.checkpoint.com

Based on Check Point Software Technologies' new Software Blade architecture and VPN-1 Power firewall, Check Point Security Gateway R70 empowers businesses with the ability to select the exact security applications they need. Whether it's firewall, VPN, IPS, anti-virus, etc., new security applications can be added as needed, reducing deployment times and operational costs.

Advanced load-sharing technology provides unprecedented performance levels and allows customers to guarantee performance by allocating resources to specific security applications. Integrated IPS uses a multi-tier intrusion prevention engine to provide strong threat control. Coupled with high performance levels, R70 provides businesses with a unique alternative to pre-emptively protect themselves against all threats without experiencing network degradation.

Security Gateway provides businesses with new levels of flexibility, simplicity and extensibility, enabling customers of all sizes to tailor network security infrastructure to meet their functional and performance needs. R70 combines security software with open systems running general purpose processors to allow customers to benefit from rapid performance improvements coming from the world's leading chip manufacturers.

In addition, it is one of the only security solutions in the market that leverages the performance benefits from multi-core architectures. Customers can deploy R70 on an open server or platform, as one of Check Point's Power-1 or IP appliances, or in virtual environments.

R70 adapts as new applications are introduced and new threats appear – delivering proactive protection for new technologies, such as VoIP or instant messaging, and against whole classes of attacks. A flexible architecture allows new solutions to be added into the gateway at will, extending the usability and extensibility of the solution. With advanced security acceleration technology, R70 ensures that enterprise information flows efficiently without compromising security. The result is an integrated firewall solution that keeps businesses safe. As part of Check Point's Unified Security Architecture, R70 integrates with other Check Point solutions to simplify security management and deployment.

BEST IDENTITY MANAGEMENT SOLUTION

Finalists 2010

- Courion for Courion Access Assurance Suite
- IBM for IBM Tivoli Identity and Access Assurance
- Quest Software for Quest One Identity Solution
- RSA, the security division of EMC, for RSA Access Manager
- VeriSign for VeriSign Personal Identity Portal

WINNER

VeriSign for VeriSign Personal Identity Portal
http://pip.verisignlabs.com

The majority of today's web users need to remember five or more passwords and PINs to access web-based email, health care and banking services, as well as a host of other services. While best practices for security dictates that web users should have no two passwords that are the same, keeping track of too many passwords has led to "password fatigue."

To alleviate this problem, VeriSign's OpenID grants access to multiple services using only one password. OpenID is a community-driven standard that is becoming a flexible method for using one set of credentials to identify users across a wide variety of sites. OpenID is user-centric. It allows users to choose how much information to share with other sites.

VeriSign Personal Identity Portal (VeriSign's OpenID offering), provides safe sign-in with one click. This allows users to sign-in to their online accounts from any computer without having to remember their username/password. Customization of a personal identity page is also offered, wherein users can share online profiles, share a video or provide links to other of their profile pages.

Extra layers of identity protection can be added to VeriSign's Personal Identity Portal to reinforce a web user's security/privacy. The VeriSign browser certificate (free) or VIP credential (low cost) provide additional security and protect web users' online identity/privacy. Access OpenID sites enable users to receive a personal identifier in the form of a URL that can be used to sign-in or register at any site that supports OpenID. This URL is the location of the user's personalized web pages.

As OpenID sees greater adoption, it is increasingly important that the OpenID provider be a trusted entity. VeriSign has been an active participant in OpenID advancement for this reason and has assisted in drafting standards, launching an OpenID provider, evangelizing the technology and developing open-source software for the marketplace.

VeriSign Personal Identity Portal benefits enterprises by helping consumers conveniently and securely login to their accounts to use online services, as well as lowering the cost of ownership as interoperable components provide maximum flexibility in solution development/deployment with less risk than a proprietary or vendor-locked solution.

BEST INTEGRATED SECURITY SOLUTION

WINNER

Symantec for
Symantec Protection Suite Enterprise Edition
www.symantec.com

Symantec Protection Suite Enterprise Edition creates a protected endpoint and messaging and web environment that is secure against today's complex malware, data loss and spam threats. Plus, it is quickly recoverable in the event of failure. The solution includes Symantec's endpoint security, messaging security and system recovery technologies that allow customers to reduce the cost of securing their environments and more effectively manage the inherent risks of today's IT infrastructures. Multiple layers of protection ensure customers are accurately identifying and addressing risks while delivering consistent protection across platforms. In the event of system loss or failure, users may recover individual files and folders in seconds, or complete Windows systems in minutes, thus minimizing downtime.

Symantec Protection Suite Enterprise Edition is unique in being able to provide the combination of multiple security and backup and recovery technologies managed by a single console. Unified management and administration across technologies eliminates deployment complexity, while flexible and scalable configuration options help organizations meet IT policy requirements and eliminate unnecessary operational tasks and their associated costs. Further, Symantec's advanced data leakage prevention and content filtering technologies ease the burden of meeting policy and regulatory objectives by automatically regulating the flow of sensitive information in email and on endpoints.

Ten years ago, a company's business information resided on a closed network, and standard anti-virus software offered adequate protection from malicious, outside attacks. The threat landscape has evolved significantly in the decade since the Melissa virus first appeared: Companies' networks are more open and accessible to partners, customers and contractors. Increasingly, the inability to recover mission-critical information promptly can spell disaster for a company in today's 24/7 business environment. Symantec Protection Suite offers a combination of security and data backup and recovery technologies in one package that's easy to install and manage, saving organizations time and money while ensuring compliance with laws and regulations governing the privacy of confidential/sensitive business information.

Finalists 2010

- Check Point Software Technologies for UTM-1 Total Security
- Juniper Networks for Juniper Networks SRX Series
- SonicWALL for SonicWALL TZ 210 Wireless-N
- Sophos for Sophos Endpoint Security and Data Protection
- Symantec for Symantec Protection Suite Enterprise Edition

BEST IDS/IPS SOLUTION

Finalists 2010

- Cisco Systems for Cisco Intrusion Prevention System
- IBM for IBM Proventia Network IPS GX6116 and IBM Proventia Network Security Controller
- SonicWALL for SonicWALL NSA E7500
- Sourcefire for Snort-based Sourcefire 3D System
- TippingPoint Technologies for TippingPoint Intrusion Prevention System (IPS)

WINNER

Cisco Systems for
Cisco Intrusion Prevention System
www.cisco.com/go/ips

The Cisco Intrusion Prevention System (IPS) protects the entire network with a range of deployment options and is able to deliver holistic network-wide security protection. This inline, network-based defense identifies, classifies and stops known and unknown threats to a network, including malware and directed attacks against servers, applications, clients and infrastructure components. Leveraging Global Correlation, Cisco IPS collaborates with tens of thousands of other security devices (including IPS, email security appliances, web security appliances) to provide fast and accurate threat protection. This advanced protection is easily deployed as a standalone appliance or as a module in a switch or router.

Cisco IPS is the only IPS with risk rating, global correlation capabilities, and the only IPS backed by Cisco Security Intelligence Operations. Cisco's patented risk rating system combines several sophisticated threat detection methods into one simple number representing the overall risk rating. It takes into account key factors, including threat origin, attack contents and target vulnerability and value. Cisco Security Intelligence Operations engages more than 500 researchers analyzing 500 GB of data from 700,000 sensors each day to detect attackers and help mitigate emerging threats. Global Correlation is Cisco's recently launched capability for IPS and enables Cisco to analyze threats from a broad range of technologies across the globe and pinpoint the source and behavior of attacks.

Intrusion detection technology has evolved to address today's complex threat environment and to meet increasing demands for security and compliance. These factors have also driven the move from pure intrusion detection capabilities to more full-featured intrusion prevention solutions. Cisco offers zero-day protection. When used with the Cisco Anomaly Detection feature, Cisco IPS can protect a network before signature updates are available, and can continue to improve protection through behavioral learning. Cisco IPS has helped customers meet compliance requirements such as PCI, *SOX*, and *HIPAA*, safeguarding companies from the expenses associated with noncompliance and data breaches. Cisco IPS offers simplified policy provisioning with Cisco's patented risk rating technology.

BEST IPsec/SSL VPN

Finalists 2010

- Astaro Internet Security for Astaro Security Gateway
- Barracuda Networks for Barracuda SSL VPN
- Citrix Systems for Citrix Access Gateway
- F5 Networks for FirePass SSL VPN
- Microsoft Corp. for Forefront Unified Access Gateway
- SonicWALL for SonicWALL Aventail EX7000

WINNER

Barracuda Networks for Barracuda SSL VPN
www.barracudanetworks.com

As the global workplace becomes increasingly mobile – IDC expects 1.9 billion users on the internet and three billion users on the phone network by 2012 – organizations require secure, clientless remote access to internal network resources from any web browser. Typical users require the use of email, file servers, intranet websites, databases and desktop access to office workstations. With conventional VPN solutions, such as IPsec or PPTP, secure access to resources is often difficult or impossible to manage. Designed for remote employees and road warriors, the Barracuda SSL VPN provides comprehensive control over file systems and web-based applications requiring external access. The Barracuda SSL VPN integrates with third-party authentication mechanisms to control user access levels and provides single sign-on.

Organizations must balance their growing remote access needs against their available IT resources, and a remote access solution must be easy to set up and maintain while having minimal impact on the IT helpdesk. By incorporating the Barracuda SSL VPN into an organization's remote access strategy, users gain the benefits of secure remote access without the cost and complexities of an IPsec solution. The Barracuda SSL VPN provides the advantages of both IPsec and SSL, integrating with popular authentication protocols, such as LDAP, and requiring no client to distribute and no additional network configurations. For IT managers, the Barracuda SSL VPN also enables IT organizations to mitigate the risks of remote access from machines they do not directly control by integrating antivirus for file uploads, verifying supported computer OS and browser version levels, and cleaning browser caches and temporary files from the computer on disconnecting from the network.

The solution is based on technology obtained through the acquisition of 3SP (based in the U.K.), the originators of the acclaimed SSL-Explorer technology. With more than 275,000 downloads of its community edition on the internet, SSL-Explorer was a highly praised and award-winning software product. After the acquisition by Barracuda Networks, this remote access technology was then integrated with Barracuda Networks' own leading antivirus management framework and hardware appliance technologies.

BEST MANAGED SECURITY SERVICE

Finalists 2010

- Google for Google Message Security, powered by Postini
- IBM for IBM ISS Managed Security Services
- McAfee for McAfee Total Protection Service
- SecureWorks for Managed Security Services
- StillSecure for StillSecure ProtectPoint

Google™ postini services

WINNER

Google for Google Message Security, powered by Postini
www.google.com/postini

More than 90 percent of email is spam and organizations need a solution that reliably and effectively stops email threats. Postini blocks more than 99 percent of spam and email threats and does so before it reaches customers' networks with a 99.99 percent uptime service level agreements (SLA). As a result, the company's customers save on bandwidth and keep spam and viruses off their infrastructure.

Because organizations want email security solutions that don't require a lot of maintenance, Postini provides email security as a service, which means that its customers don't have to install any software or hardware or perform any updates. They simply set up the service and let it do its job. As email is a key asset and organizations want to have a policy framework to manage it, Postini allows administrators to set email content policies at the global, department and/or user levels for inbound and outbound traffic. As well, customers can encrypt messages between domains using standard SSL/TLS protocols.

By stopping threats in the cloud, the solution can have an immediate impact on reducing network bandwidth needs. The tool offers real-time IP behavior analysis, and has been awarded multiple patents for pass-through technology, zero-hour virus detection, and 100 percent anti-virus SLAs.

End-users can personally configure five levels of sensitivity across six categories of spam and set their own approved/blocked senders lists.

Users plodding through spam received in their inboxes translates into lost productivity and salaries. Take the following example: A 1,000-employee company has an average salary of $65/hour. The number of workdays per year is 245 and each employee receives an average of 25 spam messages per day and spends 50 seconds finding and deleting them. If that 50 seconds for 1,000 employees is converted to annual costs, this company wastes more than $220,000 in salary and loses 211 personnel days of productivity.

Given these circumstances, Google Message Security pays for itself within 13 days. This doesn't even take into account the IT resource savings to manage spam with an in-house solution.

Google has more than 50,000 Postini customers and 15 million end-users.

BEST MESSAGING SECURITY SOLUTION

Finalists 2010

- Barracuda Networks for Barracuda Spam & Virus Firewall
- Cisco Systems for Cisco IronPort Email Security
- McAfee for McAfee Email Gateway
- Websense for Websense Email Security (Websense Hosted Email Security and Websense Email Security)

WINNER

Cisco Systems for Cisco IronPort Email Security
www.cisco.com

Enterprises of all sizes face the same daunting challenges – increasing mail volumes and new, evolving threats. The Cisco IronPort Email Security services portfolio provides customers with superior choice of deployment models built on the solid foundation of a leading email security technology. It protects 40 percent of Fortune 1000 companies from inbound threats and outbound data loss possibilities. The Cisco IronPort Email Security Portfolio addresses the needs of the market by providing email security leadership with choice, backed by guarantees. Now customers have the ability to select from an array of solutions that include an appliance form factor, a dedicated hosted infrastructure that resides fully in the cloud, a unique hybrid hosted solution with email security infrastructure both in-the-cloud and on-premises, or an on-premises managed form factor.

The tool provides end-users with a choice. Most competitors offer an appliance or a hosted service. With Cisco's solution, customers may choose the solution most suitable for their needs, and change that solution according to their needs. The dedicated infrastructure that powers all services provides customers with strong anti-spam efficacy with third party-verified 99 percent spam catch rate and less than one in one million false positive rate. Maximum data privacy is provided as users no longer have to deal with the risk of data co-mingling, advanced controls, like DLP and encryption capabilities, protect sensitive information, while real-time tools, like message tracking and reporting, make for better decision making.

The Email Security portfolio is backed by a leading Security Intelligence Operations Center (SIO). SIO features hundreds of servers, technicians and researchers analyzing terabytes of threat data each day. With this "satellite view" of the internet, Cisco often updates its products with the latest threat signatures ahead of competitors. This threat tracking system is used by the entire Cisco security portfolio, arming every level of network defense with a complete awareness of its environment. Whether the infrastructure is on premises or in-the-cloud, customers always have access to configuration and logs, real-time comprehensive reports and message tracking 24/7.

BEST MOBILE DEVICE SECURITY SOLUTION

WINNER

IronKey for IronKey Enterprise with Remote Management Service
www.ironkey.com

Security threats and compliance requirements are on the rise. With worms like Conficker maliciously winding its way through corporate networks, it is imperative that organizations implement and enforce comprehensive mobile data security polices. IronKey Enterprise with Remote Management Service combines hardware-encrypted IronKey USB flash drives with a powerful tracking and management solution. It allows organizations to remotely administer policies across thousands of IronKey Enterprise devices via the internet. IronKey Enterprise devices provide defenses that deliver layered protection to stop the spread of malware and worms. If a device is lost or stolen, it can be remotely disabled or destroyed. Enterprise requirements for protecting data, identities and online privacy are met by IronKey with this unique solution.

IronKey Enterprise devices offer strong security and help customers achieve the Federal Information Processing Standards (FIPS) 140-2, Level 3 validation. Additionally, if an IronKey is ever lost or stolen, not only is the data protected, but also through its suite of portable security applications, the data can be restored to a new IronKey from an encrypted backup.

The IronKey Enterprise with Remote Management Service works seamlessly with enterprise-level USB endpoint security management products. It provides IT administrators with centralized management and visibility across thousands of devices, ensuring that security policies are enforced. The devices include always-on hardware encryption, while intelligent anti-malware capabilities keep out malicious code. The advantages include powerful, active anti-malware protection; policy enforcement, which includes password strength, password retry limits and onboard portable applications; the ability to remotely disable or terminate lost and stolen USB drives; strong authentication with one-time password technology, such as RSA SecureID, that allows IronKey devices to be used as a two-factor token; endpoint and enterprise application integration; administrator device unlock and rest; and secure platform for virtualization.

The offering is used by commercial enterprises and government agencies and is a proven and reliable solution.

Finalists 2010

- Check Point Software Technologies for Check Point Media Encryption and Port Protection
- CREDANT Technologies for CREDANT Mobile Guardian
- IronKey for IronKey Enterprise with Remote Management Service
- PGP Corp. for PGP Mobile
- Symantec for Symantec Mobile Security Suite 5.1

BEST MULTI- AND SECOND-FACTOR SOLUTION

Finalists 2010

- Entrust for Entrust IdentityGuard
- Imprivata for Imprivata OneSign Authentication Management
- PhoneFactor for PhoneFactor
- RSA, the security division of EMC, for RSA SecurID
- VeriSign for VeriSign Identity Protection (VIP) Authentication Service

WINNER

RSA, the security division of EMC, for RSA SecurID
www.rsa.com

The RSA SecurID two-factor authentication solution reliably proves user identities through a one-time password that changes every 60 seconds. The product is used by businesses across dozens of industries to secure access to networks and other online resources. The RSA Authentication Manager software engine supports VPN gateways, web portals, Citrix installations, business applications (e.g., HR and legal), wireless (e.g., RADIUS servers), privileged user access, web single sign-on (SSO), and more. RSA SecurID tokens come in a broad array of hardware and software form factors to balance cost, risk and convenience.

RSA SecurID is interoperable with more than 375 products and platforms from more than 250 companies, making it easier to adopt within a customer's environment. RSA Authentication Manager offers on-demand authentication through SMS for business continuity. It is available via on-premise, or through MSSPs and software-as-a-service (SaaS) providers.

RSA maintains a broad reseller and distribution channel. RSA SecurID comes in a wide variety of form factors – from hardware tokens that store certificates and decrypt hard drives, to software tokens embedded in smart phones, laptops, USB drives and biometric devices.

RSA SecurID can be licensed for as few as 25 users, and the RSA SecurID Appliance option provides an SME edition with licenses starting at 10 users, making two-factor authentication accessible to organizations of all sizes. The appliance can be deployed in less than 30 minutes and is easy to maintain. It lowers TCO for organizations with fewer dedicated IT resources and distributed environments. A broad array of hardware and software tokens meets unique needs based on cost, risk and convenience. Technical benefits include an easy-to-use web interface and automated fail-over and cross-realm authentication. SMEs can also leverage a large number of RSA-licensed MSSPs and SaaS providers to reap similar benefits as those who use the appliance.

More than 30,000 organizations (covering more than 40 million users) have adopted RSA SecurID via on-premise software, appliances or hosted services. RSA commits major investments in R&D. The RSA SecurWorld channel program maintains a strong network of thousands of resellers.

BEST POLICY MANAGEMENT SOLUTION

Finalists 2010

- nCircle Network Security for nCircle Configuration Compliance Manager
- NetIQ for NetIQ Secure Configuration Manager 5.8 for Policy Management
- Novell for ZENworks Configuration Management Enterprise Edition
- SonicWALL for SonicWALL Universal Management Appliance (UMA) EM5000
- Sourcefire for Sourcefire RNA

WINNER

SonicWALL for SonicWALL Universal Management Appliance (UMA) EM5000
www.sonicwall.com

The SonicWALL E-Class Universal Management Appliance (UMA) centralizes policy management, monitoring and reporting for multiple SonicWALL appliances. The UMA provides an effective way to configure and manage global policies for security appliances and services, enhancing efficiency and providing a rapid return on investment. The appliance simplifies and automates policy management, monitoring and compliance reporting with flexible, powerful and intuitive tools. Multiple UMA devices, when deployed in a cluster, can scale to manage up to thousands of SonicWALL security appliances. This makes the SonicWALL UMA an ideal solution for small- to medium-sized businesses, enterprises and managed service providers that have either single site or distributed multi-site environments. Features include unified policy management, comprehensive monitoring and automated alerting, custom and template-based reporting, centralized logging for deep forensic analysis and remediation, secure, reliable and optimized hardware architecture, intuitive management dashboard, and high-availability services across multiple sites.

The EM5000 provides numerous advantages, including the ability to set granular policy controls from one location. It can centrally manage and define policies at a very detailed level for a large number of SonicWALL appliances. As well, central management drives efficiency gains and reduces operating expenses. The solution offers detailed and customizable reporting capabilities for compliance or other purposes.

Using these features, the IT staff benefits from increased staff productivity, streamlined management and provisioning, adherence to compliance controls, rapid response to network disruptions, high service and network uptime, and scheduled policy changes. In addition, the UMA EM5000 provides simplified inventory management, integrated service licensing, service contract co-termination, reporting for auditors and user activity reporting. This, in turn, gives the business manager greater efficiencies via a single platform, as well as relevant data for auditors, adherence to compliance controls, elimination of wasteful network usage, prevention of lapses in support coverage, and presents just one vendor to procure from.

BEST SIM/SIEM SOLUTION

Finalists 2010

- Alert Logic for Log Manager
- ArcSight for ArcSight Enterprise Security Manager (ESM)
- IBM for Tivoli Security Information and Event Manager
- Q1 Labs for QRadar SIEM
- RSA Security for RSA enVision Platform
- Tenable Network Security for Tenable's Security Center 3.4 with Log Correlation Engine 3.2
- TriGeo Network Security for TriGeo SIM

WINNER

ArcSight for
ArcSight Enterprise Security Manager (ESM)
www.ArcSight.com

ArcSight Enterprise Security Manager (ESM) is a leader in security information and event management. ESM correlates and analyzes all the log, event and transaction information generated by an enterprise's systems to find potential security threats and risks. For example, someone trying to hack into a credit card database might do three or four things that, together, look like a break-in. When ESM finds something, it notifies people so they can lock down the systems, apply patches or launch an investigation. The tool has been described as the central brain analyzing all information to secure digital infrastructure and protect business against breaches, insider threats and non-compliance risk.

ArcSight ESM was purpose-built for flexibility. Its first customers were U.S. intelligence agencies that couldn't disclose the devices they wanted to monitor, so ArcSight had to build a very flexible technology that could easily adapt to changing use cases. Some companies build technologies for specific uses in specific verticals, which produce limited architectures that are not easily adaptable or scalable.

ArcSight ESM is a leader in the market, and has broad interoperability, a flexible and powerful correlation engine and a robust ability to scale. Every major release of ArcSight's solution has introduced new capabilities that raise the bar. ArcSight has refined many of the features of its products to a second- or third-generation level based on production use.

ArcSight Enterprise Security Manager provides enterprises with complete visibility into how their entire IT investment and key assets are being used, assurance that they're being used in the intended manner, and the ability to secure digital infrastructure and achieve and remain in compliance with government and industry mandates.

Users can minimize threats and risk to enterprise information, infrastructure and operations by recognizing and responding to incidents more quickly. In addition, users can scale the solution as their needs and infrastructure grow and get an objective, neutral third party that can consolidate monitoring across other vendors' products and correlate incidents among them to surface subtle problems that are otherwise impossible to see.

BEST SECURITY SOFTWARE DEVELOPMENT

WINNER

VeriSign for VeriSign Code Signing
www.verisign.com

Developers and web publishers offer more choice and customization than ever before. Innovative applications enhance websites, mobile devices and desktop software for work and play. Everyone wants the latest application, but no one wants security or functionality compromised. How do end-users, software platforms and networks know which code to trust? Code signing from a trusted certificate authority (CA), such as VeriSign, shows the authenticated identity of the code source and proof of the content integrity. To protect software publishers and users when they download code and content over the internet and mobile networks, VeriSign Code Signing creates a digital "shrink-wrap" for code and content. VeriSign Code Signing increases the adoption and distribution of downloadable software with digital signatures, builds a trusted relationship for brands by reducing error messages and security warnings, and protects users from downloading harmful files.

VeriSign supports more platforms than any other code-signing provider with the most reliable infrastructure and the most trusted security brand on the internet. Because VeriSign root certificates come preinstalled on most end-users' devices and embedded in most applications, the digital signature authentication and verification process is seamless and transparent to most end-users. Eight out of 10 code-signing users choose VeriSign, according to an online interactive survey of software developers and decision-makers, conducted by VeriSign in July 2008. Additionally, VeriSign is the leading provider of code signing services for developers and software publishers who create applications for Microsoft platforms or participate in Microsoft Windows Logo programs.

When end-users download software signed with a VeriSign Code Signing Digital Certificate, they can be assured of the content source, as the publisher identified in the code-signing certificate is valid. They can rest assured of content integrity as the software has not been altered/corrupted since it was signed. This accountability and potential recourse serve as a strong deterrent to the distribution of harmful code. Developers benefit from VeriSign Code Signing Digital certificates because using them puts trust in their name and makes their products harder to falsify.

Finalists 2010

- Cenzic for ClickToSecure 6.0
- ClearFoundation for ClearOS
- IBM Rational Software for Ounce 6
- Mocana Corp. for Device Security Framework 5.1
- Veracode for Veracode SecurityReview
- VeriSign for VeriSign Code Signing

BEST VULNERABILITY MANAGEMENT SOLUTION

Finalists 2010

- Core Security Technologies for CORE IMPACT Pro
- eEye Digital Security for Retina Network Security Scanner
- Microsoft Corp. for Forefront Threat Management Gateway
- Qualys for QualysGuard
- Tenable Network Security for Tenable Security Center 3.4 with Nessus 4.0, Log Correlation Engine (LCE) 3.2 and Passive Vulnerability Scanner (PVS) 3.0
- TippingPoint Technologies for TippingPoint Intrusion Prevention System (IPS)

WINNER

Qualys for QualysGuard
www.qualys.com

QualysGuard provides an easy to deploy and comprehensive way to reduce security risk and meet regulatory compliance needs. All a company needs is a web browser to scan its network and applications in order to spot and fix vulnerabilities and collect compliance data. Delivered via a software-as-a-service (SaaS) architecture, the cost of QualysGuard is on average 50 to 90 percent less than traditional software scanning solutions. With QualysGuard, organizations can effectively manage their vulnerabilities and maintain control over their network security with centralized reports, verified remedies and full remediation workflow capabilities with trouble tickets. QualysGuard provides comprehensive reports on vulnerabilities and compliance issues for systems and applications, including severity levels, time-to-fix estimates and impact on business, plus trend analysis on security and compliance issues. One of its largest vulnerability management deployments is at a Fortune Global 50 company scanning more than 700,000 devices globally.

With the SaaS approach, Qualys has simplified the process of vulnerability and compliance scanning. When implementing QualysGuard, there is no infrastructure to deploy or manage. The SaaS model not only saves time and resources, but also allows managers and auditors to get a continuous view of a company's security and compliance posture. In 2009, Qualys added customer web application scanning to the QualysGuard suite allowing customers to scan for SQL injections and XSS vulnerabilities to protect their web applications against these popular attacked vectors. Also, Qualys, in partnership with VeriSign iDefense, brought immediate defenses against zero-day threats and vulnerabilities and expanded reporting capabilities, which allow for prioritized patching and real-time risk analysis. The Qualys Vulnerability Lab maintains one of the industry's largest vulnerability databases with more than 7,000 unique checks based on CVE standards. Automated signature-regression testing ensures quality security audits and daily updates for customers.

Creating an automated process to continuously monitor network and web application security and to identify vulnerabilities is critical to protecting the enterprise and maintaining regulatory compliance.

BEST WEB APPLICATION SECURITY SOLUTION

WINNER

F5 Networks for
BIG-IP Application Security Manager
www.f5.com

As more application traffic moves over the web, sensitive customer data is exposed to new security vulnerabilities and attacks, especially at the application layer. F5's BIG-IP Application Security Manager (ASM) is an advanced web application firewall that significantly mitigates the risk of loss or damage to data, intellectual property and web applications. BIG-IP ASM provides end-to-end application protection, advanced monitoring and centralized reporting, while addressing key regulatory mandates – including PCI DSS, *HIPAA*, Basel II and *SOX* – in a cost-effective way, and without requiring multiple appliances. BIG-IP ASM protects organizations – and their reputations – by maintaining the confidentiality, availability and performance of the applications that are critical to their business efforts.

In addition, because ASM offers integrated functionality with BIG-IP Application Delivery Controllers, maintenance and additional costs associated with application security are kept to a minimum without sacrificing performance. The result is one of the industry's most comprehensive web application security and application integrity solutions.

One advantage over standalone solutions is incorporating BIG-IP ASM within an Application Delivery Controller solution that can be combined with TCP optimization, L4-L7 load balancing, web acceleration and web access management services. To save time and protect application data, BIG-IP ASM comes with pre-built application security policies that provide out-of-the-box protection for popular applications, like Microsoft Outlook Web Access, SharePoint, Lotus Domino Mail Server and Oracle E-Business Financials. In addition, a built-in rapid deployment policy can quickly secure any internal or third-party application.

BIG-IP ASM also provides application protection from Layer 7 denial-of-service (DoS) and brute force attacks to address application vulnerabilities without code fixes. With the new web-scraping protection capabilities, BIG-IP ASM prevents the theft and misuse of valuable web data. Finally, the new Human Readable Policies provide offsite auditors access to a specific security policy for review to ensure maximum user productivity and streamlined auditor engagements.

Finalists 2010

- Barracuda Networks for Barracuda Web Application Firewall
- Breach Security for WebDefend
- F5 Networks for BIG-IP Application Security Manager
- TippingPoint Technologies for TippingPoint's Intrusion Prevention System (IPS)
- VeriSign for VeriSign Extended Validation (EV) Secure Sockets Layer (SSL) Certificates
- WhiteHat Security for WhiteHat Sentinel

BEST WEB FILTERING SOLUTION

Finalists 2010

- Blue Coat Systems for Blue Coat WebFilter and WebPulse Collaborative Defense
- Cisco Systems for Cisco IronPort S-Series Secure Web Gateway
- McAfee for McAfee Web Gateway
- St. Bernard Software for iPrism Web Filter
- Symantec for Symantec Web Gateway
- Websense for Websense Web Security

WINNER

Cisco Systems for
Cisco IronPort S-Series Secure Web Gateway
www.cisco.com

The Cisco IronPort S-Series web security appliance is the industry's first and only secure web gateway to combine next generation Web Usage Controls, reputation filtering, malware filtering and data security on a single platform to address the growing challenges of both securing and controlling web traffic. Leveraging Cisco SIO and global threat correlation technology help to increase the intelligence and speed of Cisco IronPort appliances. This advanced technology enables organizations to improve their security and transparently protect users from the latest internet threats.

Additionally for advanced acceptable use policy (AUP), Cisco IronPort Web Usage Controls are a leading solution for enforcing acceptable-use policies for web access, improving visibility into web traffic and raising employee productivity. This powerful solution combines a robust URL database with wide coverage in the industry and real-time dynamic categorization to identify objectionable content hidden in the dark

Cisco IronPort Web Reputation Filters analyze more than 50 different web traffic and network-related parameters to accurately evaluate the trustworthiness of a URL or IP addresses. The tool examines every request made by the browser – from the initial HTML request to all subsequent data requests, including live data, which may be fed from different domains. This gives these filters an advantage over vendors that reduce web reputation to a simple URL filtering category.

The Cisco IronPort Anti-Malware System enables the Cisco IronPort S-Series the ability to offer multiple anti-malware scanning engines on a single, integrated appliance. This system leverages the Cisco IronPort Dynamic Vectoring and Streaming (DVS) engine, as well as verdict engines from Webroot and McAfee, to provide protection against the widest variety of web-based threats.

Its coupling to other Cisco products will allow this solution to absorb value from the traditional endpoint and the traditional firewall markets – a $10 billion combined market today. The trend toward borderless network blurs the distinctions of these separate markets, and the resulting re-definition of value will be the third albeit longer-term growth vector for the Cisco IronPort S-Series business.

BEST SECURITY COMPANY

Finalists 2010
- BigFix
- Fortify Software
- IBM Corp.
- McAfee
- Qualys

WINNER

IBM Corp.
www.ibm.com/security

IBM has been an industry leader for nearly 50 years, helping CxOs and IT professionals secure their corporate infrastructures with solutions that go beyond just collections of niche products. IBM's customers rely on the planet's most secure databases, applications, operating systems, storage and servers. IBM offers comprehensive security solutions and services addressing compliance, applications, data, identity and access management, networks, threat prevention, systems security, email, encryption, virtualization and cloud security.

Through an end-to-end approach to security across people and identity, data, applications, infrastructure, compliance and the physical infrastructure, IBM's security capabilities are among the top in the industry. With multiple leadership awards in market presence and technology innovation, IBM is able to offer more than 120 security products and the experience of over 15,000 researchers, developers and SMEs focused on security initiatives.

IBM clients gain the benefit of integrated, security solutions that reduce the cost and complexity of managing security solutions from multiple vendors.

IBM's world-class security support services provide the technical and operational expertise needed to maximize security investment. By providing a global network of support centers to assist customers worldwide, often in their native language, IBM partners with its customers around the clock to solve any implementation and technical issues.

This support is available regardless of client location or implementation method of hardware, software and/or managed security services. IBM provides a variety of support levels – from self-help to tiered levels – enabling customers to choose the one that best meets their needs. IBM is recognized for its outstanding customer support and consistently high customer satisfaction.

The company has staked a firm claim in the security marketplace and emerged as a market leader capable of meeting any global organization's security needs through an integrated, diverse and flexible portfolio of products and services across key industries.

With a strong, deep and broad security portfolio, IBM is in a strong position, able to leverage its considerable assets and reputation and provide innovative technologies and intellectual property that address both today's vulnerabilities and newly emerging threats.

ROOKIE SECURITY COMPANY OF THE YEAR

WINNER

HyTrust
www.hytrust.com

HyTrust delivers an enterprise-class solution – the first offering of its kind – aimed at solving a critical issue that currently hampers the broader adoption of virtualization throughout the enterprise. HyTrust emerged from stealth mode some six months ago and is currently involved in numerous proof-of-concept deployments at some of VMware's largest enterprise accounts.

HyTrust enables the broader adoption of virtualization – and all the business advantages that come with it – by providing a single point of control for hypervisor policy definition, access control and security configuration. This process enables virtual infrastructure to become as operationally ready as physical infrastructure.

The company recently demonstrated its offering at VMworld 2009 and left the show with Best Security Product and Best of Show accolades. In addition, Hytrust was one of the top winners in *SC Magazine*'s Security Innovators Throwdown, a competition to find young security companies with fresh ideas, held during the SC World Congress in October 2009.

HyTrust is the only type of solution in its category. Other vendors offer pieces of the puzzle (e.g., dedicated access control or configuration management or logging), but no vendor provides all these capabilities in one package that is specifically dedicated to policy enforcement within virtual infrastructure. Although HyTrust has only been generally available for about six months, the company is clearly posed to be a leader in this area.

HyTrust provides 24/7/365 phone support for all critical issues. The company offers two types of maintenance and support programs: Software Maintenance and Platinum Support is offered for the Enterprise Edition and is required at the time of purchase, renewable on an annual basis. Software Maintenance and Forum Support is offered for the Community Edition. One of the key drivers behind Community Edition is to enable small- and medium-sized businesses (SMB) to cost-effectively gain the same features and benefits for their virtualized environments as their counterparts in the largest enterprises. Community Edition enables large enterprises to quickly and easily evaluate HyTrust appliance capabilities in their environments.

HyTrust aims to build a community of professionals who are committed to growing the reach of cloud-based computing services and expanding the use of virtualization throughout their organizations.

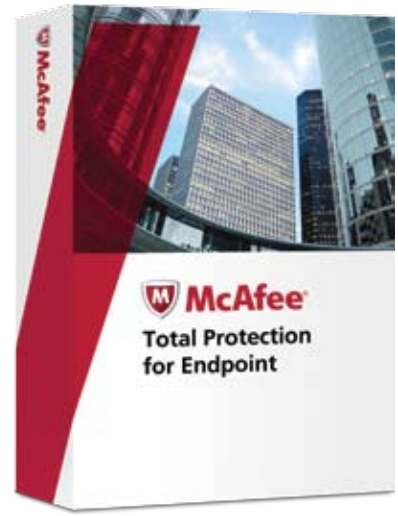
Finalists 2010

- AccelOps
- Allgress
- Damballa
- HyTrust
- StrikeForce Technologies

BEST ENTERPRISE SECURITY SOLUTION

Finalists 2010

- McAfee for McAfee Total Protection for Endpoint
- Protegrity for Protegrity Data Protection System 5.0
- SonicWALL for SonicWALL NSA E7500
- Sophos for Sophos Endpoint Security and Data Protection
- Websense for Websense Web Security Gateway



WINNER

McAfee for McAfee Total Protection for Endpoint
www.mcafee.com

A leading pure-play company, McAfee has more than 60 million endpoints under enterprise management (not including consumer). The company has experienced 18 consecutive quarters of double digit year-over-year growth.

McAfee professional services – including consulting, product education and award-winning technical support – help customers make the most out of their McAfee solutions and keep protection up-to-date. The company works with highly trained and experienced partners to help customers optimize its solutions. To supplement its partner services, McAfee Foundstone Professional Services brings an objective perspective and a unique combination of tools and training to help identify and implement the most effective solutions for meeting particular needs. At McAfee Customer Service and Technical Support, certified security specialists provide support with a wealth of knowledge and resources. Support options include 24/7/365 access.

McAfee Avert Labs is a top-ranked research organization with more than 350 researchers on four continents. The McAfee Avert Labs blog offers a view into up-to-the-minute security research. Using global threat intelligence, McAfee Avert Labs works 24/7 to anticipate and defend against the next wave of malware.

McAfee has been awarded more than 439 patents and many more patents are pending. Patents allow the company to build superior solutions, defend innovations and generate licensing revenue.

Total Protection for Endpoint enables companies to lower their overall cost of managing endpoint security with a completely integrated management console, ePolicy Orchestrator (ePO). The advanced proactive security of anti-spyware and host IPS helps stop zero-day threats before outbreaks cause damage and downtime.

MSI International, a leading global recruiting firm, completed a survey of 488 ePO and non-ePO users and found that ePO users spend 38 percent less time on security reporting; spend 41 percent less time developing security policies; manage 30 percent more endpoints; use 50 percent less hardware; and that admins save about six hours per week.

BEST REGULATORY COMPLIANCE SOLUTION

Finalists 2010

- Archer Technologies for GRC Solutions
- e-DMZ Security for TPAM Suite
- Modulo for Modulo Risk Manager
- Qualys for QualysGuard PCI
- SenSage for SenSage 4.5 Event Data Warehouse
- Vanguard Integrity Professionals for Vanguard Audit and Compliance Solution

WINNER

e-DMZ Security for TPAM Suite
www.e-dmzsecurity.com

e-DMZ Security has a strong customer base – with more than 350 customers in more than 17 countries, including many of the world's largest enterprises in several verticals. Despite the current economic conditions, e-DMZ Security has seen continued growth and rapid acceptance of its Total Privileged Access Management (TPAM) solution with a 75 percent growth in the first half of 2009 versus the second half of 2008.

The company offers 7/24/365 hotline access via phone, email and support portal as part of its standard support package, as well as product updates/patches and next-day appliance replacement. It offers this level of service via a global support center located in Raleigh, N.C., along with extensive and growing international sales and support partners. e-DMZ Security also has depots located in the United States, Europe and Asia to best support appliance replacement services globally.

Innovation is at the forefront of what drives e-DMZ Security. This is proven based on its past product portfolio and continues based on current directions. The company was one of the first to develop and deliver a commercial off-the-shelf (COTS) solution specifically designed to meet security and compliance requirements for the lifecycle management of privileged passwords – e.g., password auto pepository (PAR) in 2003. Innovation continued with the release of eGuardPost (2005) as a product focused to manage/control privileged sessions, including full-session recording and DVR replay of access to Unix, Windows, web applications and more. The recent release/announcement of the company's TPAM suite (2009) represents a leading solution that from a single appliance platform provides privileged password management, session management/control/recording and command management/delegation. With TPAM, companies can add required functions to meet changing compliance needs/audits by enabling additional modules. Areas of continued innovation include: real-time session monitoring, full hand-held workflow and extended user provisioning.

The company's mission is to enhance security and compliance in today's global enterprise by providing quality, innovative and customer-driven solutions to control and audit elevated rights access within the enterprise and extended community.

BEST SME SECURITY SOLUTION

Finalists 2010

- Astaro Internet Security for Astaro Security Gateway
- Imprivata for OneSign
- Kaspersky Lab for Kaspersky Open Space Security
- Reflexion Networks for Reflexion Total Control (RTC)
- Sentrigo for Hedgehog Enterprise
- WatchGuard Technologies for Firebox X Core

WINNER

Astaro Internet Security for Astaro Security Gateway
www.astaro.com

Especially in the security space, new technologies directly influence what customers require in a product. Ever-changing technology leads to a high feature turnover rate – something that was extremely hot last year, but does not look so exciting now because it is either required and assumed in all security solutions or it has fizzled out. While trade shows and industry musings do have an impact in development, Astaro tends to focus directly on the customer and partner as opposed to volatile market fads.

Astaro recently introduced the Astaro Feature Request Site, which allows partners, customers and employees to make suggestions for improvements and enhancements. As a testament to Astaro's commitment to providing the features its customers need, more than 70 percent of the features requested on the request site were included in the recent release of version 7.5 of the Astaro Security Gateway.

Astaro's mission is to help small- and medium-sized businesses secure their networks and to meet the business needs of SMBs. Introducing the Feature Request site has allowed Astaro to better understand customer needs, and with the introduction of the Astaro Security Gateway 625 model and version 7.5 of the Astaro Security Gateway, the company is meeting the needs of partners and customers even better than before.

According to estimates, such as those provided by firms like IDC, and internal sales analysis, Astaro Security Gateway currently enjoys a seven percent market share worldwide in the UTM space.

Astaro offers 24/7 call-in customer support. Additionally, Astaro offers a central repository of all manuals, technical articles and other helpful documents; an Up2Date service, which provides information about the latest Astaro technical updates; a quick-start guide to help organizations install and configure their Astaro Security Gateway; a hardware compatibility list; and a tool that enables users to check any URL and verify its categorization via Astaro's Secure Web feature.

Astaro has achieved 26 percent quarter-over-quarter growth for the second quarter of 2009. This growth also represents a 16 percent increase in revenues over the second quarter of 2008 and marks Astaro's 14th consecutive quarter of growth, as well as the company's third most profitable quarter to date.

BEST SECURITY TEAM

Finalists 2010

- eBay
- Cargill
- Diebold Enterprise Security Team
- Southwest Washington Medical Center
- Troy University IT Security Team

WINNER

eBay
www.ebay.com

Dave Cullinane, the CSO at eBay, and his top-level management team lead by example with an incredible pairing of expertise and work ethic. They have created a world-class security team that is highly integrated with the business. eBay's state-of-the-art security practices are an optimal combination of people, process and technology. It is a team that not only focuses on securing eBay, but on securing the entire internet.

As the world's leading online marketplace, eBay's main product is trust. The company's security team has established itself as a critical enabler of a trusted marketplace by proactively engaging with internal departments, partners and customers to identify opportunities to reduce fraud and prevent security incidents from ever occurring.

While many security teams are reactive to security incidents, eBay works to secure the future of the business every day. As an example, eBay's security team keeps ahead by leveraging emerging technologies, like Zscaler's SaaS web security and other cloud-based security services. When eBay must pursue criminal hackers, it does so with a combination of world-class tools, innovative partnering and a relentless commitment to the mission. The infamous hacker Vlad "Vladuz" Duiculescu was apprehended by Romanian authorities as the result of an eBay-led coalition that included the FBI, U.S. Secret Service, Department of Justice, and Department of State, among others.

Cullinane and his security team are driven by ROI metrics, and are advanced in their use of risk analytics. eBay is able to accurately predict the amount of fraud reduction and cost savings that will result from an investment in information security resources. eBay also takes a leading role in supporting community-based security initiatives. The company understands that achieving a more secure internet is a shared responsibility. To achieve this, eBay encourages a spirit of cooperation and shares incident information with peers. Its huge online footprint allows it to often identify dangerous malware prior to anyone else; and it openly shares this information, even with competitors. eBay is also noted for hosting educational events for a cross-section of Silicon Valley companies. Cullinane encourages his team to stay involved in all major security associations and events to help move the industry forward.

CSO OF THE YEAR

Photo by Kent Lacin

WINNER

Mark Weatherford, CISO, office of information security, state of California
www.cio.ca.gov/ois

California government is a vast organization employing 225,000 people distributed across more than 130 agencies, departments, offices and boards. With the establishment of the office of information security, under the leadership of Mark Weatherford, there has been renewed emphasis on protecting the state's enterprise IT assets through a centralized, focused, action-oriented security program. Weatherford developed and manages a strong security team – a Herculean feat in the decentralized bureaucracy of California government – through a combination of personal leadership, enterprise policy guidance and operational outreach and training. One example of how he forged a sense of teamwork among California's 128 ISOs is the enterprisewide security policy refresh. The results of this project standardize security policies across California. The collaboration implicit in this project began a migration in the state from a collection of individuals carrying out their missions to a group of professionals focused on enterprise security.

Prior to the appointment of Weatherford as California's CISO, the state government's business lines approached information security in a decentralized fashion. An integral part of Weatherford's effort in California is managing the cultural change necessary to transfer from an ad-hoc to an enterprise organization. Weatherford pursues a strategy to facilitate this change by gaining the trust and sponsorship of business and IT executives throughout the state. One example of this sponsorship is the May 2009 Governor's Reorganization Proposal (GRP). The reorganization, proposed by Gov. Arnold Schwarzenegger and approved by the legislature, folded the CISO position and office of information security into the office of the state chief information officer. Weatherford was integral in the planning and negotiations that ensured that placement, a clear sign to California's business leaders of the importance the governor is placing on information security.

Weatherford proselytizes for information security within and outside of California state government – promoting the CISO as an enterprisewide position with over-arching security responsibilities – while heightening the profile of information security across government.

Finalists 2010

- Dave Cullinane, eBay
- Bobby Dominguez, Catalina Marketing Corp.
- Robert Maley, state of Pennsylvania
- Bill McQuaid, Parkview Adventist Medical Center
- Mark Weatherford, state of California

BEST PROFESSIONAL CERTIFICATION PROGRAM

Finalists 2010

- GIAC - Global Information Assurance Certification for GIAC Security Essentials Certification (GSEC)
- GIAC - Global Information Assurance Certification for GIAC Certified Forensics Analyst (GCFA)
- Information System Audit and Control Association for Certified information Security Manager (CISM)
- (ISC)² for CISSP
- (ISC)² for SSCP

WINNER

(ISC)² for CISSP
www.isc2.org/cissp

Known as the gold standard of information security certifications, the Certified Information Systems Security Professional (CISSP) was the first certification accredited by the American National Standards Institute (ANSI) to International Standards Organization (ISO) Standard 17024:2003. The CISSP is not only an objective measure of excellence, but a globally recognized standard of achievement. It requires at least five cumulative years of relevant work experience in two or more of the 10 domains of the CISSP CBK (common body of knowledge), or four years of work experience and a four-year bachelor's degree or a master's degree in information security. To maintain the certification, CISSP holders are required to obtain 120 continuing professional education (CPE) credits every three years, with a minimum of 20 CPEs posted during each year of the three-year certification cycle. This continuing education ensures that CISSP-certified pros are keeping up with the latest threats.

One major point that sets the CISSP apart from other security certifications is the breadth of knowledge and experience necessary to pass the exam. A CISSP candidate cannot specialize in just one domain. They must know and understand the full spectrum of the (ISC)² CBK to become certified. In addition to the required five cumulative years of relevant work experience in two or more of the 10 domains, CISSPs must also legally adhere to the (ISC)² Code of Ethics, be endorsed by a current (ISC)² member, and undergo continuing education to keep the certification current. By meeting each of the above requirements, employers can rest assured that when they hire a professional who holds the CISSP credential, that person has been tested on understanding industry best practices and possesses a broad knowledge of the field and sound professional ethics and judgment.

A professional who holds the CISSP typically develops information security strategy, writes information security policy, manages information security and personnel, and ensures security policy is complying with industry regulations. Further, concentrations of the CISSP are available for those desiring additional validation of skills in management (CISSP-ISSMP), architecture (CISSP-ISSAP) and engineering (CISSP-ISSEP). These concentrations allow CISSPs to focus their talents on functional areas of importance to them or their companies.

BEST PROFESSIONAL TRAINING PROGRAM

WINNER

SANS Institute for SANS Training
http://sans.org

The SANS Institute is the leading organization in information security training and is known for providing intensive, immersion training designed to help students master the practical steps necessary for defending systems and networks. The SANS Institute's mission is to teach practical knowledge and hands-on skills that can be applied to real-world, everyday scenarios. At the heart of SANS are the many security practitioners in government agencies, corporations and universities around the world who invest hundreds of hours each year in research and instruction to help the entire information security community.

SANS courses are hands-on and full of technical exercises versus theory-based lectures. Students will be able to apply the knowledge they learned in class immediately on returning to the office. All courses are developed by administrators, security managers and information security professionals who are real-world practitioners in the field applying these best-case practices everyday.

More than 15,000 students a year attend SANS information security training. Diverse course offerings and expert instructors offer a unique learning experience and deliver true technical skills that students can use every day in their jobs. SANS courses are continually updated so content is current and includes active exploits. Students who train with SANS return for further training and recommend courses to their co-workers and friends.

In addition to top-notch training, SANS offers certification via the ANSI-accredited Global Information Assurance Certification (GIAC), a security certification program, as well as numerous free security resources.

The GIAC validates the real-world skills of IT security professionals. GIAC's purpose is to provide assurance that a certified individual has practical security awareness, knowledge and skills in key areas of computer security, network security and software security. GIAC offers certifications for more than 20 job-specific responsibilities that reflect the current practice of information security.

GIAC certification is held in high regard because it measures specific knowledge areas instead of general purpose information security knowledge. Additionally, once certified, a certificant can strengthen their skills set at the higher levels of gold and expert status.

Finalists 2010

- (ISC)² for (ISC)²
- SANS Institute for SANS Institute
- The Training Camp
- Vanguard Integrity Professionals for Vanguard Enterprise Security Training and Education

EDITOR'S CHOICE AWARD

WINNER

National Cyber-Forensics and Training Alliance
www.ncfta.net/main/home/

Headquartered in Pittsburgh, the National Cyber Forensics & Training Alliance (NCFTA) was created with the mission of facilitating collaboration between private industry, academia and law enforcement to identify, mitigate and neutralize complex cyber-related threats.

In May 2009, President Obama's administration composed a 60-day review to assess U.S. policies and structures for cybersecurity. The review considered a number of effective public-private partnerships and cited the NCFTA as an "effective model," which "has a clearly defined institutional mission, well-defined roles and responsibilities for participants, and a clear value proposition that creates incentives for members to participate."

At present, the NCFTA coordinates several initiatives, including the "Clean Credit" initiative, where it acts as the industry's common meeting space and information collection and distribution point for key fraud detection indication variables.

Another project, the Digital PhishNet, is a joint partnership between the NCFTA and Microsoft, established in 2004 as a collaborative mitigation and neutralization operation to unite industry leaders in technology, banking, financial services and online retail services with law enforcement to combat "phishing."

In order to address the serious and growing problem of illicit online pharmaceutical sales, the NCFTA established the Pharmaceutical Fraud Initiative, in partnership with several U.S. and international pharmaceutical companies and government agencies. The focus of this initiative is mitigation and dismantlement of affiliate networks through providing a forum to exchange information regarding emerging and ongoing threats to the pharmaceutical industry.

In addition, NCFTA has partnered with online retailers, financial institutions, the Merchant Risk Council and the National Retail Federation to mitigate and neutralize frauds specifically targeted at retailers and shipment companies.

Another area of focus has been working with the key shippers to reach agreement among these interested and related parties to establish an information-sharing protocol, whereby internet protocol (IP) addresses involved in shipping fraud will be centrally collected at the NCFTA and will be made available to these entities for e-channel mitigation through authentication controls.

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.scmagazineus.com