February 14, 2017 • San Francisco

#scawards
Calling out admirable work

The cybersecurity industry seems on the cusp of impactful evolutionary change. Make no mistake, we’ve come far. But now more than at any time before, we seem at a tipping point of sorts.

Average consumers believe the companies with which they do business should be doing all they can to protect their sensitive data and privacy. Our current president is talking about ‘the cyber’ and requirements for securing it. Industry experts wonder if in 2017 we’ll see the first nation-state cyberattack acknowledged as an act of war.

At the same time, though the industry itself is still somewhat nascent with its inconsistent hierarchical reporting structures and differing cybersecurity titles from company to company, it is finding its place. Some practitioners and other executive types believe 2017 finally will see CISOs and the like getting that much overdue seat at the boardroom table.

Yes, we probably are facing a tipping point. And it will either see organizations embracing cybersecurity as an enabler and differentiator to their organizations or witness them continuing to coast with hopes intellectual property won’t be breached.

Our SC Awards Program, here and in the U.K., celebrates those who understand cybersecurity and their organization’s role in it, who aren’t just coasting. As well, we call out all the vendors, service providers and insurgent organizations supporting these and other efforts to continually advance the field.

By acknowledging the efforts of IT security practitioners, rookie and long-standing product and service providers that support them and the many professional organizations that provide help along the way, we strive to play our part in fighting back the sometimes wearisome and difficult happenings the industry faces. For us, showcasing to your colleagues, bosses, everyday consumers and still others that cybersecurity pros like you play vital roles in keeping virtually every internet-connected activity and business – in fact, the global economy – up and running for us all is an honor. And, whether information security is on the brink of some wider grand acceptance and acknowledgment of need or not, we intend to continue calling out admirable work and industry advances for years to come.

– Illena Armstrong, VP, editorial, SC Media
The Aflac family congratulates

TIM CALLAHAN
Senior Vice President of Global Security

for being named an SC Awards 2017 finalist in the CSO of the Year category. This is another fine feather in your cap.
SC Awards 2017

The Judges

CO-CHAIR
Ilenna Armstrong
VP, editorial, SC Media

CO-CHAIR
John Johnson
global security architect of a Fortune 100 company

Roota Almeida
head, information security, Delta Dental of NJ

Ron Baklarz
CISO, Amtrak

Nick Belov
director, MUFG

Vikas Bhatia
CEO, Kalki Consulting

Fernando Blanco
VP and CISO, CHRISTUS Health

Joshua Bregler
senior director of security, AMAG Pharmaceuticals

John Bruggeman
CTO, Hebrew Union College

Chris Bunton
director, infrastructure/ISO, HHSC DADS

Christopher Burgess
CEO, Prevenadra

Miki Calero
founder, Urbis Global

Chris Camacho
CEO, NinjaJobs

Vaune Carr
CSO, CCG

Michael Castro
senior director, information security and risk management, Loblaw Companies

Benjamin Caudill
CEO, Rhino Security Labs

Jaime Chanaga
chairman/president, Counter Global Defense

Ken Clegg
VP of technology, CashLINQ

Daniel Crothers
CIO, Brand Ventures

Michael Dent
CISO, Fairfax County Government

Matthew Deren
senior security engineer, Belk

Uday Deshpande
CISO, TATA Motors

Rick Doten
chief, cyber and information security, Crumpton Group

Patricia Edfors
VP, information security, privacy and compliance, Sirius XM Radio

Karen Evans
national director, U.S. Cyber Challenge

Jane Frankland
managing director, Cyber Security Capital

Pamela Fusco
CFO, ISSA

Ajit Gaddam
chief architect, VISA
The Judges

Mike Gibbons
CISO, Edward Jones

Terry Gold
founder, D6 Research

Stuart Golding
managing director, UK Data Secure

Stacey Halota
VP, information security and privacy, Graham Holdings Company

Vincent Hamm
president, Aim High!

Mansur Hasib
cybersecurity technology, The Graduate School

Erin Jacobs
founding partner, Urbane Security

Ashutosh Kapse
head of information security & technology risk, IOOF Holdings

Aaron Kirby
SVP authentication solutions, MasterCard

Jonas Kriks
CIO, ATEL

Cedric Leighton
chairman, Cedric Leighton Associates

Daniel Lieber
president, Innovative Ideas Unlimited

Gary Long
VP, solutions & services, GT Global Network

Jon Longstaff
head of cybersecurity, OMNITRIC Group

Ryan Loy
CIO, ADTRAN

Jim Maloney
CISO, AvidXchange

Richard Marshall
CEO, X-SES

Erin Nealy Cox
board director, Sally Beauty

Travis Paakki
director of application development and systems integration, Portland Public Schools

Christopher Paidhrin
CISO, city of Portland

Mitchell Parker
executive director, information security & compliance, Indiana University Health

Neil Passingham
founder/director, GardPass Cyber Security

Daniel Polly
director, enterprise information security, First Financial Bank

Michael Raeder
CISO, Orbital ATK

Jason Raymond
CISO, Guidewell Mutual Holding

Todd Redfoot
CISO, GoDaddy

Jamie Rees
senior cybersecurity strategist, NB Power

Sandi Roddy
senior cyber analyst
The Judges

Randolph Sanovic
owner, RNS Consulting

Steve Santorelli
director of analysis and outreach, Team Cymru

John Sapp Jr.
CISO, Orthofix

Jay Schulman
principal, RSM US

Bobby Singh
CISO, Toronto Stock Exchange

Nathan Smolenski
VP, CISO, Spencer Stuart

Daniel Srebnick
owner, Technical Merits

Jeff Stark
information security officer, Ontario Pension Board

Richard Starnes
CISO, Kentucky Health Cooperative

Roberta Stempfley
director, MITRE

Priscilla Tate
founder & director, TechForum

Dennis Thibodeaux
technical instructor and security SME, New Horizons Learning Group

Richard Timbol
CISO, Davis Polk & Wardwell
THE BREACH STOPS HERE™

90% of all enterprises are moving to the cloud, billions of users are accessing data across millions of applications. All accessed by one simple permission. The password.

The results? Two thirds of enterprises have been breached due to compromised passwords. Until now.

Centrify is a massive rethink in security, defending today’s boundaryless hybrid enterprise through the power of identity services.

THIS IS NEXT DIMENSION SECURITY

WWW.CENTRIFY.COM
SC Media thanks all sponsors for their generous support of the SC Awards 2017. Their involvement has made possible this event, which helps raise professional standards in the information security industry worldwide.

Aflac
Aflac is a Fortune 500 company providing financial protection to more than 50 million people worldwide. When a policyholder or insured gets sick or hurt, Aflac pays cash benefits fast. For six decades, Aflac voluntary insurance policies have given policyholders the opportunity to focus on recovery, not financial stress.

Barracuda
Barracuda simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide, cloud and hybrid deployments.

Centrify
Centrify is a leader in securing enterprise identities against cyber-threats that target today’s hybrid IT environment of cloud, mobile and on-premises. Centrify helps protect against the leading point of attack used in data breaches by securing an enterprise’s apps and infrastructure for all its users.

Forcepoint
Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people’s intent as they interact with critical data. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance.

ID Watchdog
ID Watchdog provides identity theft protection and resolution services as an employee benefit. ID Watchdog leverages proprietary technology that searches billions of data points to detect and alert changes in the personal identity profiles of our subscribers.

LogRhythm
LogRhythm empowers organizations to rapidly detect, respond to and neutralize damaging cyberthreats. The company’s patented award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, user entity and behavior analytics (UEBA), security automation and orchestration and advanced security analytics.

Proofpoint
Proofpoint protects your people, data and brand against advanced threats and compliance risks. Built on the cloud and the world’s most advanced intelligence platform, our solutions help you effectively detect and block targeted attacks and respond quickly to suspected compromises.

Sentinel One
SentinelOne was founded by a group of international defense and intelligence experts who saw the need for a dramatic new approach to endpoint protection. The SentinelOne Endpoint Protection Platform (EPP) offers real-time, unified endpoint protection, driven by machine learning and dynamic behavioral detection.

Splunk
Splunk is a market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk software provides the enterprise machine data fabric that drives digital transformation. More than 12,000 customers in over 110 countries use Splunk solutions in the cloud and on-premises. Splunk products include Splunk Enterprise, Splunk Cloud, Splunk Light and premium solutions.
Web & Email Security
Next Generation Firewall
Insider Threat Solutions
Data & IP Loss Prevention
Cross Domain Solutions

VISIT US AT
BOOTH #3527
Welcome from the co-chairman

Never has it been more exciting or more difficult to be a cybersecurity professional. The pace of change is rapid, and we must always be learning and adapting as we compete in an asymmetrical war against our adversaries.

In the past year, we saw significant regulatory change and we face uncertainty in light of changes to EU privacy laws, Safe Harbor rules, BREXIT and the changes a new U.S. administration may bring to privacy, commerce and regulations. We are fortunate to see strides being made with industry information-sharing groups, and we continue to mature our security programs as we tie our policies and controls to standard frameworks.

As well, corporate security teams are more business-minded, forward thinking and are receiving support from the board level. Cybersecurity leaders in our organizations have not only the technical knowledge, but the business acumen to have earned their place at the table with other executives. The SC Awards recognizes highly successful teams and industry leaders for the work that they are doing to raise the bar for our industry and to set an example that we should all aspire to.

The cybersecurity market continues to grow, innovate and mature. As our organizations face new threats, new regulatory requirements and adopt new technologies, they now have vendor solutions that enable business growth and add business value. Terms such as artificial intelligence, machine learning and threat hunting have become a part of our vocabulary. Flexible solutions that are cloud-ready and integrate with our legacy systems help make the task of protecting data, reducing risk and defending against threats – wherever our data may reside – achievable, adaptable and affordable.

The SC Awards 2017 recognizes vendors and practitioners who make a difference by offering innovative solutions to effectively and efficiently inform us about threats and vulnerabilities, protect our data and keep it confidential, and detect, respond and recover from cyber attacks.

As co-chair of the SC Awards 2017, I am humbled to be involved in the process to select and honor the leaders and innovators to receive awards in the many categories we designate as crucial to the success of our industry. I applaud your efforts, your diligence and your success in delivering the best our cybersecurity industry has to offer. You make an important difference every day in bringing trust and security to our interconnected world.

– John Johnson, advisory board member, SC Media

Trust Award
BEST ADVANCED PERSISTENT THREAT (APT) PROTECTION

WINNER
Check Point Software Technologies for SandBlast

Check Point SandBlast stops unknown malware, zero-day and targeted attacks from infiltrating networks. SandBlast is based on patented CPU-level exploit detection technology to identify threats earlier, before malware has an opportunity to deploy evasion code. With its unique inspection capabilities, SandBlast delivers the highest catch rate for threats, and stops malware that can usually bypass first-generation sandboxes using evasion techniques.

SandBlast also includes Threat Extraction, allowing practical protection by proactively reconstructing content into safe documents, preventing malware from ever reaching users. With first-generation sandboxing products, customers had to make a choice to either delay delivery of files until inspection was complete, or to run in a detection-only mode, letting content through while testing was done in parallel. Threat Extraction makes real-world deployment in prevent mode possible by promptly delivering a clean copy of content, and then only providing access to the original once it is deemed safe.

By detecting the exploit, rather than traces of the malware that follows it, this patented technology leaves the attacker with no place to hide, detecting attacks that would otherwise be missed by first-generation sandboxing solutions.

Check Point SandBlast Zero-Day Protection identifies more malware, and actively blocks it with minimal impact on user delivery times. SandBlast offers cutting-edge sandboxing capabilities to detect threats before evasion techniques can be used, making this solution the best line of defense against undiscovered exploits, zero-day and targeted attacks.

Finalists 2017
- Check Point Software Technologies for SandBlast
- Cisco for Advanced Malware Protection
- CrowdStrike for Falcon
- Proofpoint for Targeted Attack Protection (TAP) for Email
- SonicWALL for Capture Advanced Threat Protection
Trust Award
BEST BEHAVIOR ANALYTICS/ENTERPRISE THREAT DETECTION

WINNER
CrowdStrike for Falcon

CrowdStrike continues to set the standard in both threat prevention and detection, using signatureless machine learning and behavioral-based analytics. CrowdStrike earned a 100 percent efficacy rating on its first public test, according to results published by SE Labs, which is certified by AMTSO for detecting both known and unknown samples of malware with a false positive rate of zero percent. CrowdStrike prevention capabilities continue to excel with the development of new behavioral exploit prevention indicators of attacks (IOA) to provide further protection against sophisticated browser-based exploits, in addition to its broad existing capabilities in pre-execution exploit mitigation techniques. Specifically, a groundbreaking new malware-free intrusion prevention IOA is now in place to protect organizations against web shell-based attacks. The IoA approach allows the technology to detect adversaries that remain undetectable by the rest of the industry by identifying malicious actions and intentions (stealing credentials, executing commands, etc.)

To analyze billions of events swiftly and accurately in real-time, machine learning models require a level of computational power and scalability that is only possible with a fully SaaS-based architecture. As Falcon collects more threat intelligence and identifies attacks, this information is turned into a new detection and learned by the algorithm, and deployed across its cloud network so all endpoints are protected – sending the bad actors back to the drawing board. From a business perspective, companies not only have access to a solution that stops all breaches but also scales with the needs of the business without friction or disruption.

Finalists 2017
• CrowdStrike for Falcon
• Imperva for Counterbreach
• Rapid7 for InsightIDR- Escape Alert Fatigue, Relentlessly Hunt Threats
• SentinelOne for Endpoint Protection Program
• Splunk for UBA 3.0 (User Behavior Analytics)

Trust Award
BEST CLOUD COMPUTING SECURITY SOLUTION

WINNER
Vera for Vera Security

Even the most sophisticated enterprises can’t guarantee how 100 percent of their confidential information is shared. Modern file sharing and communication tools facilitate collaboration and productivity, but the moment confidential data is shared outside an organization, enterprises lose all visibility and control over who, how and where data travels. To address this challenge, Vera secures information directly, anywhere it travels, no matter how it’s shared (e.g., email, Dropbox, Box, Office365), and especially after it’s downloaded or removed from corporate systems (intentionally or by clumsy users). With Vera’s dynamic data protections, organizations can secure, track and even revoke access to sensitive information, even after it’s passed through the perimeter. And, just as importantly, Vera makes securing data simple, seamless and invisible. Through its content- and storage-agnostic platform, Vera secures any type of digital information, including Office documents, PDFs, JPG images, movie files and proprietary file types, anywhere they’re stored. Vera enables IT to protect, govern and manage the transmission of information without impacting the way employees and external parties collaborate. Vera can secure any type of file across any device or application, without requiring end-users to install additional software, agents or proprietary plug-ins to access secured information. With native integrations to Office 365, Box, Dropbox and Okta, Vera automatically and invisibly protects files without impacting employee productivity.

On the technical side, Vera makes it possible for security teams to establish strong encryption of content the default, not the exception.
Trust Award
BEST COMPUTER FORENSIC SOLUTION

WINNER
Guidance Software for EnCase Forensic and EnCase Endpoint Investigator

With EnCase, Guidance Software created the category for digital forensic investigations and has provided market-proven and legally indisputable solutions for law enforcement and corporate investigations for more than 20 years.

EnCase Forensic and EnCase Endpoint Investigator provide a powerful, judicially accepted platform that serves as the foundation for corporations, government agencies and law enforcement to conduct digital investigations of any kind. As market pioneers, Guidance knows the complexities of criminal investigations and what it takes to get to case closed. When the stakes are high, law enforcement needs a powerful, court-proven solution.

EnCase Forensic and EnCase Endpoint Investigator deliver the most powerful investigation products on the market, allowing organizations to improve efficiency and effectiveness of their staff, while maintaining the breadth and depth of visibility. New capabilities include: built-in investigation workflows to speed training, predefined search criteria for the most common inquiries to enable time-saving automated search, simplified reporting, quick preview capabilities, and integration with project VIC to save law enforcement investigators time when completing child exploitation examinations.

From HR issues, compliance violations, regulatory inquires, IP theft, and more, Endpoint Investigator delivers 360-degree visibility across endpoints, no matter where they are.

Digital forensic investigators require tools that keep pace with evolving adversaries and that allow them to complete endpoint investigations quickly and effectively. With regular updates, EnCase Endpoint Investigator and EnCase Forensic deliver the most powerful investigation products on the market, allowing organizations to improve efficiency and effectiveness of their staff, while maintaining the breadth and depth of visibility. New capabilities include: built-in investigation workflows to speed training, predefined search criteria for the most common inquiries to enable time-saving automated search, simplified reporting, quick preview capabilities, and integration with project VIC to save law enforcement investigators time when completing child exploitation examinations.

Trust Award
BEST DATA LOSS PREVENTION (DLP) SOLUTION

WINNER
Digital Guardian for Data Loss Prevention

Digital Guardian (DG) for Data Loss Prevention (DLP) offers next-generation data protection, purpose-built to stop accidental and malicious data loss by insiders and outside attackers. With Digital Guardian’s acquisition and completed integration of Armor5 for cloud data protection, and Code Green Networks for data discovery, classification and network DLP, DG for DLP is now the most well rounded DLP solution available today. It is the only solution on the market that prevents data loss at the endpoint, network and in the cloud, leveraging the same endpoint agent, network sensor and management console, thus streamlining the level of effort and number of resources required to manage an effective data security program.

Digital Guardian is a recognized “Leader” in Gartner’s 2016 Magic Quadrant for Enterprise DLP and was rated number one in intellectual property protection.

The core business advantage to DG for DLP is the consolidation of security capabilities into a single data protection platform. DG for DLP is the only platform that provides:

- Network, endpoint and cloud data loss prevention – leveraging the same management console, same endpoint agent and same network sensor
- Protection from well-meaning and malicious insiders and outside attackers. Competitive DLP solutions continue to focus on protecting data for the insider or compliance use case only. DG for DLP is the only solution that has extended capability to prevent data loss by outside attackers too – leveraging the same technology. To match this capability, buyers would need to purchase two or three different technologies from competitors.
- Flexible deployment options, including on-premise, as a managed service or as a hybrid of the two.

Finalists 2017

- Forcepoint for SureView Insider Threat
- Guidance Software for EnCase Forensic and EnCase Endpoint Investigator
- Infoyte for HUNT
- LogRhythm for Network Monitor
- Symantec for Blue Coat Security Analytics Platform

Finalists 2017

- Bitglass for Data Leakage Prevention for the Cloud and Mobile Era
- Digital Guardian for Data Loss Prevention
- Forcepoint for AP-DATA & AP-ENDPOINT
- Safetica North America for Safetica 7
- Spirion for Sensitive Data Manager

Yuval Eldar, president, Secure Islands
CUSTOMERS LOVE US
(apparently, industry analysts do too)

COMPLETE IDENTITY PROTECTION
From benefit plans for the Fortune 500 to individual consumer protection, we’ve become an industry leader in prevention, detection and resolution of identity theft. And our customer service is recognized as the best in the industry.

1.866.513.1518 | idwatchdog.com
Trust Award
BEST DATABASE SECURITY SOLUTION
WINNER
HexaTier for Unified Database Security and Compliance Solution

Organizations need complete, flexible and easy-to-install security and compliance solutions, especially for the cloud and next-generation (DBaaS). Traditional solutions tools cannot support cloud or DBaaS as they are costly to implement, take significant time to install and must be physically attached to the database, limiting implementation options. Enterprises also need a solution to support their infrastructure today and in the future.

HexaTier’s unified database security and compliance solution offers a patented reverse proxy technology that secures databases across multiple platforms: DBaaS, private, public or hybrid cloud environments and on-premise. Installation takes minutes. HexaTier acts as a front-end to the database and works as a reverse proxy, effectively hiding and securing the database. It scans the database for sensitive information to ensure regulatory compliance, automatically setting auditing and masking policies. HexaTier examines queries and responses, securing them in both directions, making it the perfect tool for database security.

The reverse proxy-based solution takes only a few minutes to implement, reduces the database attackable surface, offers a complete database firewall and prevents SQL injections. Its automatic detection and classification of sensitive data (SSN, PII, emails, passwords, etc.) as well as its segregation of duties ensures alignment with regulatory requirements. It dynamically masks sensitive data accessed from application screens, reports, development and DBA tools and ensures that developers, testers and admins can access production and non-production databases without exposing sensitive data.

HexaTier is the only solution on the market that supports next-generation because of its reverse-proxy technology.

Trust Award
BEST EMAIL SECURITY SOLUTION
WINNER
Proofpoint for Proofpoint Email Protection

Proofpoint Email Protection stays ahead of new and emerging threats through ongoing innovation and ever-increasing threat intelligence. The 2016 threat landscape has featured a combination of malware and malware-free threats. Proofpoint has maintained accurate detection and protection against both types of threats.

To prevent BEC, Proofpoint introduced dynamic impostor email classification in early 2016, and DMARC enforcement and reporting in mid-2016 with the acquisition of Return Path’s Email Fraud Protection Business Unit. New security response capabilities enable automated retraction of malicious emails found in end-user inboxes, removing the threat. Proofpoint Email Protection integrates inbound email security with outbound filtering and encryption, secure file share and email continuity. Delivered as a cloud-based SaaS offering, dedicated/virtual appliance, software or hybrid, Proofpoint delivers consistent functionality and performance regardless of deployment.

Proofpoint Email Protection centralizes the tasks of improving email security and protection, controlling confidential and regulated data and ensuring business continuity. With accurate malware detection and blocking, coupled with spear-phishing and BEC protection, Proofpoint Email Protection drastically reduces potential information loss and financial consequences due to infection and compromise.

In addition, automated remediation actions remove potentially malicious email from inboxes to add another layer of protection, without requiring additional management overhead. Proofpoint’s DLP capabilities also automatically detect a wide variety of private information and block, quarantine or apply encryption as appropriate and customized by the customer.

Finalists 2017
• HexaTier for Unified Database Security and Compliance Solution
• Imperva for SecureSphere
• Netwrix Corporation for Netwrix Auditor
• Protegrity for Database Protector
• Vormetric for Data Security Platform

Finalists 2017
• Cisco for Email Security Solution
• IRONSCALES for IronTraps
• Mimecast for Secure Email Gateway
• Proofpoint for Proofpoint Email Protection
• Trustwave for Secure Email Gateway
Trust Award
BEST FRAUD PREVENTION SOLUTION

WINNER
Distil Networks for Distil Networks

Distil Networks takes a proactive, comprehensive approach to stopping online fraud and serves customers in industries spanning e-commerce, travel, digital publishing and many more. For each customer, defense against bots starts at the perimeter with good web application security hygiene. Distil inspects each HTTP request in real time, determines if it’s a malicious bot, then gives customers the option to CAPTCHA or block the request outright. Machine learning algorithms then learn legitimate traffic patterns to pinpoint dangerous anomalies. Customers can also turn on more aggressive settings across critical attack vectors like account registration forms and login screens. By incorporating Distil Threat Intelligence, customers can also identify high-risk transactions in real time, evaluate the need for a review, or deny the transaction.

Distil provides visibility into what bots are doing on a website, who are behind those bots, and how much they’re costing the business. Specific safeguards include: protection against reconnaissance attacks, man-in-the-browser attacks, brute-force attacks and application denial of service. Additionally, companies are able to protect their brand by preventing content theft, data mining and negative SEO attacks. For e-commerce sites, they are able to halt online fraud in real time including payment fraud, carding, account hijacking, as well as new account fraud. As APIs provide more connectivity between applications, Distil acts as an automatic shield against API hijacking, scraping and abuse. Distil offers flexible deployment, offering cloud CDN or physical or virtual appliances and doesn’t require changes to underlying web infrastructure.

Distil customers benefit from a proactive defense posture supported by a machine-learning infrastructure that analyzes attack patterns in real time.

Finalists 2017
- Distil Networks for Distil Networks
- Pindrop for Phoneprint
- Proofpoint for Email Fraud Defense
- RSA Security for RSA Adaptive Authentication for eCommerce
- Terbium Labs for Matchlight

Trust Award
BEST IDENTITY MANAGEMENT SOLUTION

WINNER
CyberArk for CyberArk Privileged Account Security Solution

The CyberArk Privileged Account Security Solution pioneered the way organizations manage, secure and protect privileged accounts. The identity and access management industry is typically focused on two areas – managing identities (business enablement) and managing access. That access control piece is becoming an increasingly important component of security and risk management programs.

With CyberArk’s layered approach, based on its Shared Technology Platform, CyberArk offers proactive protection and real-time threat detection that extends identity management beyond human users to also include application identities. The CyberArk Enterprise Password Vault features a master policy engine that enables customers to set, manage and monitor privileged account security policy in a single, simple, natural language interface.

To effectively manage all privileged identities, accounts used by commercial-off-the-shelf (COTS) applications and custom-in-house applications must also be considered. Many organizations often overlook the fact that these applications are also granted administrative privileges to access many assets on the network. CyberArk Application Identity Manager, part of the CyberArk Privileged Account Security Solution, enables organizations to protect critical business systems by eliminating hard-coded credentials from application scripts, configuration files and software code, and removing SSH keys from servers where they are used by applications and scripts.

SC Magazine highlighted CyberArk as a five-star product, noting its ease-of-use, security-focused development approach and seamless ability to integrate with existing IT environments.

Finalists 2017
- CA Technologies for CA Identity Suite
- Centrify for Identity Service
- CyberArk for CyberArk Privileged Account Security Solution
- SecureAuth for IDP
- SSH Communications Security for Universal SSH Key
When a major restaurant franchise brand with 8,000 locations wanted to roll out managed security services in each store, it turned to Trustwave for threat management – the largest single managed security services (MSS) deployment ever. Looking for brand protection, compliance, scalable network security and management (at an affordable price), it turned over security to Trustwave so it could focus on growing its business. With Trustwave, the chain was able to achieve compliance and bolster security within their budget. They now have a security “extension” to their IT team that keeps each location safe from cybercrime 24/7/365. This is a prime example of how Trustwave Managed Security Services helps SMEs – including restaurants, hotels and other types of businesses – fight cybercrime, protect data and reduce risk. Gartner recognized Trustwave as the fastest-growing MSSP, and IDC recently named Trustwave a Leader in the IDC MarketScape.

The global shortage of experienced security professionals coupled with the rapidly increasing pace of advanced threats by cybercriminals has created a “perfect storm” that most companies are finding increasingly difficult to navigate. Trustwave’s managed security services offers broad-based security expertise 24/7/365 at a fraction of the cost it would take to maintain a similar capability in house. This allows businesses to scale and respond rapidly to changing threat conditions, leveraging the global technical expertise of Trustwave’s security analysts who, more often than not, have already dealt with a particular threat or exploit previously somewhere else before the typical customer is even aware that the threat exists. This frees up the customer to focus on core business initiatives and with Trustwave’s assistance ensures that the solution is implemented securely from the start.

Finalists 2017

- Digital Guardian for Managed Security Program
- Radware for Attack Mitigation Service
- Rapid7 for Analytic Response
- SecureWorks for Managed Security Services
- Trustwave for Trustwave Managed Security Services

Trustwave for Trustwave Managed Security Services

When a major restaurant franchise brand with 8,000 locations wanted to roll out managed security services in each store, it turned to Trustwave for threat management – the largest single managed security services (MSS) deployment ever. Looking for brand protection, compliance, scalable network security and management (at an affordable price), it turned over security to Trustwave so it could focus on growing its business. With Trustwave, the chain was able to achieve compliance and bolster security within their budget. They now have a security “extension” to their IT team that keeps each location safe from cybercrime 24/7/365. This is a prime example of how Trustwave Managed Security Services helps SMEs – including restaurants, hotels and other types of businesses – fight cybercrime, protect data and reduce risk. Gartner recognized Trustwave as the fastest-growing MSSP, and IDC recently named Trustwave a Leader in the IDC MarketScape.

The global shortage of experienced security professionals coupled with the rapidly increasing pace of advanced threats by cybercriminals has created a “perfect storm” that most companies are finding increasingly difficult to navigate. Trustwave’s managed security services offers broad-based security expertise 24/7/365 at a fraction of the cost it would take to maintain a similar capability in house. This allows businesses to scale and respond rapidly to changing threat conditions, leveraging the global technical expertise of Trustwave’s security analysts who, more often than not, have already dealt with a particular threat or exploit previously somewhere else before the typical customer is even aware that the threat exists. This frees up the customer to focus on core business initiatives and with Trustwave’s assistance ensures that the solution is implemented securely from the start.

Finalists 2017

- Digital Guardian for Managed Security Program
- Radware for Attack Mitigation Service
- Rapid7 for Analytic Response
- SecureWorks for Managed Security Services
- Trustwave for Trustwave Managed Security Services

When a major restaurant franchise brand with 8,000 locations wanted to roll out managed security services in each store, it turned to Trustwave for threat management – the largest single managed security services (MSS) deployment ever. Looking for brand protection, compliance, scalable network security and management (at an affordable price), it turned over security to Trustwave so it could focus on growing its business. With Trustwave, the chain was able to achieve compliance and bolster security within their budget. They now have a security “extension” to their IT team that keeps each location safe from cybercrime 24/7/365. This is a prime example of how Trustwave Managed Security Services helps SMEs – including restaurants, hotels and other types of businesses – fight cybercrime, protect data and reduce risk. Gartner recognized Trustwave as the fastest-growing MSSP, and IDC recently named Trustwave a Leader in the IDC MarketScape.

The global shortage of experienced security professionals coupled with the rapidly increasing pace of advanced threats by cybercriminals has created a “perfect storm” that most companies are finding increasingly difficult to navigate. Trustwave’s managed security services offers broad-based security expertise 24/7/365 at a fraction of the cost it would take to maintain a similar capability in house. This allows businesses to scale and respond rapidly to changing threat conditions, leveraging the global technical expertise of Trustwave’s security analysts who, more often than not, have already dealt with a particular threat or exploit previously somewhere else before the typical customer is even aware that the threat exists. This frees up the customer to focus on core business initiatives and with Trustwave’s assistance ensures that the solution is implemented securely from the start.

Finalists 2017

- Digital Guardian for Managed Security Program
- Radware for Attack Mitigation Service
- Rapid7 for Analytic Response
- SecureWorks for Managed Security Services
- Trustwave for Trustwave Managed Security Services

When a major restaurant franchise brand with 8,000 locations wanted to roll out managed security services in each store, it turned to Trustwave for threat management – the largest single managed security services (MSS) deployment ever. Looking for brand protection, compliance, scalable network security and management (at an affordable price), it turned over security to Trustwave so it could focus on growing its business. With Trustwave, the chain was able to achieve compliance and bolster security within their budget. They now have a security “extension” to their IT team that keeps each location safe from cybercrime 24/7/365. This is a prime example of how Trustwave Managed Security Services helps SMEs – including restaurants, hotels and other types of businesses – fight cybercrime, protect data and reduce risk. Gartner recognized Trustwave as the fastest-growing MSSP, and IDC recently named Trustwave a Leader in the IDC MarketScape.

The global shortage of experienced security professionals coupled with the rapidly increasing pace of advanced threats by cybercriminals has created a “perfect storm” that most companies are finding increasingly difficult to navigate. Trustwave’s managed security services offers broad-based security expertise 24/7/365 at a fraction of the cost it would take to maintain a similar capability in house. This allows businesses to scale and respond rapidly to changing threat conditions, leveraging the global technical expertise of Trustwave’s security analysts who, more often than not, have already dealt with a particular threat or exploit previously somewhere else before the typical customer is even aware that the threat exists. This frees up the customer to focus on core business initiatives and with Trustwave’s assistance ensures that the solution is implemented securely from the start.
Trust Award

BEST MULTIFACTOR SOLUTION

WINNER

RSA Security for RSA SecurID Access

Identity is today’s most consequential attack vector. Compromised identities are exploited at every stage of the cyber kill chain. Verizon’s “2016 Data Breach Investigations Report” cites that compromised identities are involved in 63 percent of breaches. Organizations need identity controls that create hurdles for attackers and mitigate identity risk, minimizing damage and loss.

Not having the visibility into the users of all of your critical applications – traditional enterprise, cloud, mobile and web – or the ability to set a common security control across these applications, can leave organizations unprepared for a sophisticated attack. RSA SecurID Access delivers secure and convenient access for any user, from anywhere, to anything. Organizations use RSA SecurID Access to regain control of a disrupted perimeter with strong, secure access and single sign-on to the leading web and SaaS applications, native mobile apps and traditional enterprise resources (including VPNs, firewalls, etc.).

RSA SecurID Access offers centralized management, standard and customized reporting options, advanced notifications, software token QR code provisioning, pre-packaged integration services, bulk user upload capabilities, the RSA Ready Program which includes 400+ fully supported technology integrations, and a variety of authenticator options based on user needs. RSA offers 24/7 Customer Support in multiple languages, and access to product guides and FAQs. Dedicated Technical Support and Professional Services resources are available with Project Managers for special implementation requirements. In the Premium edition, RSA SecurID Access employs a hybrid approach where all sensitive information is kept on premise while users securely authenticate. No passwords are ever copied to the cloud.

Trust Award

BEST NAC SOLUTION

WINNER

Cisco for Cisco Identity Services Engine (ISE)

Employees today demand access to work resources from more devices and through more nonenterprise networks than ever before - even IoT devices need access. As the network expands, the complexity of letting people access the right network resources and applications, maintaining device and behavioral visibility, and controlling risk grows. The potential impact of failing to identify and remediate security threats grows exponentially.

Cisco ISE simplifies the complexity of secure network access. Organizations gain awareness of everything hitting their network and get consistent, efficient network access.

Get ahead of secure access violations and breaches with superior visibility and dynamic controls – visibility into the users and devices accessing your network and the control to help ensure that only the right people from the right devices get the correct access to the enterprise services.

Cisco Identity Services Engine enables you to control all access throughout the network from one place, simplifying access delivery across wired, wireless, and VPN connections. You can also see user and device details showing who and what is on the network – details that strengthen security and enable better and faster decisions with these user and device insights. You can stop and contain threats by dynamically controlling network segmentation. As a controller for Cisco TrustSec, ISE provides a simple, scalable way to manage segmentation across the network - using the network devices already in place to enforce segmentation and access control policies. This allows you to easily update security policy settings, limit unnecessary network exposure, and prevent threats from compromising your network in real time.

Finalists 2017

• Cisco for Cisco Identity Services Engine (ISE)
• F5 Networks for F5 BIG-IP Access Policy Manager (APM)
• ForeScout for CounterACT
• Hewlett Packard Enterprise for Aruba ClearPass
• IntelliGO Networks for Network Access Control

Finalists 2017

• CensorNet for SMS Passcode
• Easy Solutions for DetectID with Biometric Authentication
• Gemalto for SafeNet Authentication Service
• iovation for Customer Authentication
• RSA Security for RSA SecurID Access
Trust Award
BEST RISK/POLICY MANAGEMENT SOLUTION

WINNER
Tenable Network Security for SecurityCenter Continuous View

With SecurityCenter Continuous View (CV), Tenable provides a comprehensive view of security and compliance posture in real-time, eliminating security gaps through complete visibility, actionable context and threat prioritization, and continuous assurance that security and compliance are aligned with organizational goals.

Customers are able to measure their adherence to industry standards and regulatory mandates.

SecurityCenter CV provides customizable Assurance Report Cards (ARCs) that CISOs can use to define and measure security assurance, including adherence to security policies, on a continuous basis. ARCs enable customers to express security policies in a business context, and assess them continuously for security assurance. The ARCs also allow security teams to identify the gaps where policies are failing to meet business objectives, and make the changes necessary to improve.

Security and IT teams no longer have to piece together disconnected snapshots of assets, vulnerabilities and threats. SecurityCenter CV integrates intelligence from vulnerability assessment, threat information, log analysis and continuous network monitoring to deliver a complete view of enterprise security, corporate risk and compliance status. Security and IT can implement a comprehensive control framework that is common to multiple security frameworks and compliance regimes. Tailored reports, dashboards and ARCs meet specific reporting formats.

The ARCs enable security leaders to define their security program objectives in clear and concise terms, identify and close potential security gaps, and communicate the effectiveness of their security investments to C-level executives, board members and business managers.

Best Risk/Policy Management Solution Finalists 2017
• Bay Dynamics for Risk Fabric
• SolarWinds for Network Configuration Manager
• Tenable Network Security for SecurityCenter Continuous View
• Tufin for Network Orchestration Suite
• Venafi for Trust Protection Platform

Trust Award
BEST SIEM SOLUTION

WINNER
Hewlett Packard Enterprise for ArcSight Enterprise Security Manager (ESM) and ArcSight Data Platform (ADP)

ArcSight has protected enterprises for over a decade, evolving over years as a SIEM market leader (Gartner MQ 2016 for SIEM).

As organizations scale, they rely on intelligent security operations to maintain the integrity of their security posture. ArcSight addresses sophisticated attacks, needs for quick resolution under shortage of security personnel, and data volume, variety and velocity needs due to expanding attack surface.

ArcSight Data Platform (ADP)’s open architecture supports the use of data by third-party applications such as Hadoop, data lakes and proprietary in-house applications. It collects data from any source and enriches it with security context, consolidates the information for maximum storage and retrieval efficiency. ArcSight Enterprise Security Manager (ESM) is a powerful enterprise security management software for analyzing and correlating every event that occurs, enabling customers to get a quick and accurate picture of users, apps and data to predict, protect and respond to attacks in real-time.

Deployment cost is lower given ArcSight’s reduced hardware footprint from efficient compression and high ingestion rates. ArcSight Event Broker acts as a data hub, collecting information at one million events/second. ArcSight Logger can support large SOC operations by allowing 100 concurrent searches. ArcSight is the only open architecture SIEM solution in the market and is better equipped for SOC use cases where multiple products from different vendors are used. By embedding Kafka-based Event Broker, ArcSight collects and sends data anywhere, empowering customers to leverage existing solutions/in-house applications.

Best SIEM Solution Finalists 2017
• Bay Dynamics for Risk Fabric
• SolarWinds for Network Configuration Manager
• Tenable Network Security for SecurityCenter Continuous View
• Tufin for Network Orchestration Suite
• Venafi for Trust Protection Platform

• Splunk for Enterprise Security 4.5 (ES) with Adaptive Response
We can help. LogRhythm’s Threat Lifecycle Management (TLM) platform empowers your team to detect and respond to cyber attacks—fast. It delivers the ability to “see” broadly and deeply across your entire IT environment, so your team can evaluate alarms, investigate threats, and respond to incidents—all in a single interface. With embedded user and entity behavior analytics (UEBA) and security automation and orchestration (SAO), your team will work more efficiently and more effectively to protect your organization from today’s most concerning threats.

Start monitoring your network for threats today: logrhythm.com/freemium

They will get in. They can be stopped.
Trust Award

BEST UTM SECURITY SOLUTION

WINNER
SonicWALL for Dell SonicWALL TZ Firewall Series

Companies of all sizes are overwhelmed by the sheer volume of network traffic and require security solutions that secure the business from today’s emerging threat landscape. With the wrong firewall, the business is susceptible to costly hits including multi-million dollar remediation expenses and immeasurable brand damage.

For SMBs, the SonicWALL TZ Firewall Series delivers enterprise class security capabilities for small business budgets. Built around state-of-the-art, multi-core security processors and integrated 802.11ac wireless controller, the SonicWALL TZ series provides a complete wireless network security solution. By including wireless in the security perimeter, organizations can separate guest users from employees. The SonicWALL TZ Wireless Firewall Series enables SMBs to be sophisticated security users without having a large IT staff. These firewalls allow SMBs and distributed enterprises to realize the benefits of enterprise-class 802.11ac wireless performance and security, with a simple network set-up and management console.

Weak, outdated firewalls and intrusion detection systems are blind to modern encrypted threats, giving cybercriminals a clear path to slip malware into the network and wreak havoc. Network performance and user productivity plummet when the firewall chokes under compute-intensive operations such as decrypting and inspecting SSL traffic. Secure wireless connectivity should enable the business by boosting productivity for employees, enhancing customer satisfaction and increasing sales at a cost less than deploying a wired infrastructure.

While many organizations struggle with the concern that increasing security will result in a poorly performing network, the SonicWALL TZ Series is easy to install and manage.

Finalists 2017
• 5nine Software for Cloud Security
• Entensys for UserGate UTM
• SonicWALL for Dell SonicWALL TZ Firewall Series
• Sophos for UTM
• WatchGuard Technologies for FireBox T70

Trust Award

BEST VULNERABILITY MANAGEMENT SOLUTION

WINNER
Barracuda for Barracuda Vulnerability Manager

Data breaches remain a top concern for organizations of all sizes. Whether a global enterprise or a small business, web application vulnerabilities can disrupt operations, lead to costly data breaches and erode customer trust. Often, maintaining application security can be complex and expensive; however, this cost pales in comparison to the damage that can be done. The Barracuda Vulnerability Manager, offered free of charge to Barracuda customers, enables administrators to easily identify and remediate web application vulnerabilities.

As a cloud service, Vulnerability Manager identifies all common web application vulnerabilities, such as those on the OWASP Top 10, including SQL injection, crosssite scripting, and others. However, its major technical advantage is its ability to remediate vulnerabilities with a single click by integrating with a Web Application Firewall, and to monitor the status of previously applied fixes by viewing logs, audit trails and configuration information.

From a business standpoint, Vulnerability Manager is free to use for Barracuda customers, meaning any organization can easily understand how they are vulnerable and how they can secure themselves. Organizations can choose to use the Barracuda Web Application Firewall for easiest integration, or export data to six other WAF vendors.

Finalists 2017
• 5nine Software for Cloud Security
• Black Duck for Hub
• Core Security for Core Vulnerability Insight
• RiskSense for RiskSense Platform
• Synack for Crowd Security Intelligence

From a technical standpoint, Barracuda Vulnerability Manager identifies all common web application vulnerabilities, such as those on the OWASP Top 10, including SQL injection, crosssite scripting, and others. However, its major technical advantage is its ability to remediate vulnerabilities with a single click by integrating with a Web Application Firewall, and to monitor the status of previously applied fixes by viewing logs, audit trails and configuration information.

From a business standpoint, Vulnerability Manager is free to use for Barracuda customers, meaning any organization can easily understand how they are vulnerable and how they can secure themselves. Organizations can choose to use the Barracuda Web Application Firewall for easiest integration, or export data to six other WAF vendors.
**Trust Award**

**BEST WEB APPLICATION SOLUTION**

**WINNER**

Imperva for Imperva Web Application Firewall (WAF)

Verizon’s “2016 Data Breach Investigations Report (DBIR)” states that web application attacks are the number one cause of data breaches. Web application solutions should: Stop the sheer volume and variety of attacks, including technical attacks, abuse of function and credential compromise; provide non-invasive deployment and protection for apps’ footprints on-premises in-the-cloud syndicated from partners and external entities; and enhance operational efficiency by providing highly-accurate protection without false positives or disruption to legitimate traffic.

Imperva Web Application Firewall (WAF) delivers an advanced web application solution and fits seamlessly into physical, virtual and cloud-based data centers. The Imperva solution stops business logic, DDoS and technical attacks, including those from the OWASP Top-10, from exploiting web applications; learns baseline application behavior and automatically adapts security policies to application footprint changes to protect against vulnerabilities; and correlates attacks through intelligence services, crowd-sourced from customers and curated by the Imperva Defense Center for high accuracy.

For an unprecedented, consecutive third-year, Imperva is the only vendor in the Gartner Magic Quadrant leader’s quadrant for Web Applications Firewalls. It provides accuracy of detection. With unique capabilities, like dynamic profiling and correlated attack validation, customers gain the highest detection accuracy and lowest false positives/negatives.

It was first to market with regular signature updates, crowd-sourced threat intelligence, IP reputation services, bot mitigation and account takeover protection.

A philosophy of protecting apps without changing them and of deploying WAF without changes to architecture.

---

**Excellence Award**

**BEST CUSTOMER SERVICE**

**WINNER**

Webroot for Webroot SecureAnywhere

Webroot offers a variety of documentation and resources that focus on deployment and management of its products. These include quick guides for getting started (online and downloadable PDFs), including full user manuals that have sections dedicated to multiple options of deployment and management and a complete service manual accessible from within the product. A Webroot education channel on YouTube offers an instructional series of videos on getting started and using the products – including deployment and management.

An online knowledge base contains FAQs for troubleshooting.

Webroot offers free, 24/7 telephone support to all of customers. The company has implemented a “follow-the-sun” strategy with support offices in each major region – APAC, EMEA and the Americas. Customers can contact via phone, email or open tickets directly from the agent. “Critical” and “Major” issues have a target response time of less than four hours and less than six hours, respectively. For “Medium” and “Normal” level support cases, the company targets a response time of less than eight and 24 hours, respectively.

Webroot supports an active and collaborative online community where customers can get involved in discussions about the product, general IT security concerns, ask questions and submit feature requests. The community is moderated by Webroot employees who will weigh in on topics to make sure the discussions are valuable, organized and appropriate. The company also has a FAQ section of its site which uses a series of questions to provide assistance. Both of these resources are available free of charge to all customers.

Given that its product is cloud-based, Webroot customers typically do not require on-site assistance. However, in certain circumstances, it can be arranged at no extra cost.

---

**Finalists 2017**

- Barracuda for Web Application Firewall
- Contrast Security for Contrast Enterprise
- F5 Networks for F5 BIG-IP Application Security Manager (ASM) and F5 Silverline Web Application Firewall
- Imperva for Imperva Web Application Firewall
- Prevoty for Runtime Application Security

---

**Finalists 2017**

- Avecto for Defendpoint
- Barracuda for Customer Support
- ID Watchdog for Platinum
- Proofpoint
- Webroot for Webroot SecureAnywhere
Excellence Award
**BEST EMERGING TECHNOLOGY**

**WINNER**
Exabeam for Exabeam User Behavior Intelligence Platform

Exabeam’s User Behavior Analytics (UBA) technology “connects the dots” across a user’s activities to detect if stolen credentials are being used to attack a corporate network. As part of the expected ~$9 billion solutions market, Exabeam is designed to notify security analysts when anomalous behavior takes place.

Historically, SIEM products would be the assumed solution for this problem. However, attacks have changed, shifting from network-based to identity-based, and SIEM products continue to miss them, allowing breaches to occur and failing to help security operations center (SOC) teams respond effectively.

Exabeam detects identity-based attacks and helps SOC staff respond quickly and completely after detection. It uses machine learning to automatically create a unified identity for each user, across all of that user’s IP addresses, devices and accounts. It then creates per-user baselines of normal behavior and compares activity to that baseline to determine anomalies and then prepares a timeline for guided response.

Exabeam’s technology uses machine learning to map normal human behavior patterns in order to identify suspicious activity, pinpoint the riskiest cyberthreats and find the imposters within the organization’s infrastructure before they can make off with its data.

It enhance compliance reporting. Companies have policies regarding access and attribution of access rights. Exabeam provides attribution of the unauthorized access to the person using the credential at the time.

Further, it accelerates response. Security incidents can take six to 10 days to piece together investigation information about accounts compromised and systems affected. Exabeam can eliminate one week per incident of analyst time.

---

Excellence Award
**BEST ENTERPRISE SECURITY SOLUTION**

**WINNER**
Splunk for Splunk Enterprise Security

Splunk has experienced unparalleled growth rates and in 2016 was named a leader in Gartner’s SIEM Magic Quadrant for the fourth consecutive year. Customer growth for Splunk Enterprise Security (ES) continued to expand across FY2016, with security now accounting for roughly 40 percent of Splunk’s business. For Splunk’s last fiscal year report, ending February 25, 2016, the company reported $220 million in revenue, up 49 percent year-over-year. Last quarter, Splunk announced over 500 new customers, increasing total customer count to over 12,000 in over 110 countries, compared to around 7,900 customers as of July 2015. This growth is a reflection of the value Splunk generates for its customers as its big data architecture supports the convergence of security and many different use cases for enterprise operational intelligence.

The company offers customers a variety of professional services and has offices around the globe to ensure, fast, localized support. For customers with support contracts, P1 issues are responded to immediately. Splunk Education offers a wide range of customer classes that cover installation, administration, advanced searches and more. Splunk offers a full set of public, easily searchable, technical publications covering all Splunk products (all the documentation can be exported for offline use as well). Splunk also has a vibrant online community on answers.splunk.com – this is a Splunk-moderated forum with thousands of registered users and tens of thousands of questions. Many questions are answered within minutes of being posted.

A superior TCO is why many organizations adopt Splunk solutions to replace their traditional security solutions. Lower TCO comes from deployment flexibility, simplicity of expansion and upgrade to big data scale.

---

**Finalists 2017**
- Cylance for CylancePROTECT
- Exabeam for Exabeam User Behavior Intelligence Platform
- Flashpoint for Flashpoint Platform
- Javelin Networks for Javelin ZeroMove
- Trusona for Cloud Identity Suite

---

**Finalists 2017**
- Carbon Black for Cb Response
- CrowdStrike for Falcon
- Cylance for CylancePROTECT
- LogRhythm for Security Intelligence and Analytics Platform
- Splunk for Splunk Enterprise Security
Excellence Award
BEST REGULATORY COMPLIANCE SOLUTION

WINNER

Proofpoint for Proofpoint Information Protection, Archive, and Compliance

Proofpoint protects some of the largest brands in the world. Over 2,000 customers use Proofpoint compliance solutions, with roughly a 20 percent year-over-year growth rate.

At the heart of digital communications is email, with social media increasing in role. Proofpoint provides the visibility and controls to help organizations keep communications compliant, identify sensitive information at rest across the network, and retain communications for compliance in regulated sectors across the globe.

Based on customer feedback, Proofpoint’s customer service is highly differentiated from its competition. Regular third-party surveys measure customer loyalty and satisfaction. Most recently, Proofpoint scored well above industry average in all categories surveyed, with a 95 percent satisfaction rating.

Proofpoint believes that commitment to the customer doesn’t end with initial solution(s) purchase. Customer support is available 24/7/365 online, with complimentary 24/7 telephone support for priority issues. The support portal provides access to white papers, a robust knowledge base, online help and communities, and case management.

Customers can access training and become a Proofpoint Accredited Engineer through a self-paced course. Multiple levels of service are available to meet customer’s business needs. These include proactive service, account and support oversight, special case handling and insight into security issues, as well as a deeper view into the threat landscape and more.

Customers benefit from lower TCO using Proofpoint compliance due to predictable costs. Irrespective of data quantity created, archived, monitored or scanned, pricing is per user or per account per year.

Excellence Award
BEST SECURITY COMPANY

WINNER

CrowdStrike

In 2016 alone, CrowdStrike opened offices internationally in EMEA and APAC and doubled its employee base.

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. It collects 14 billion events per day across 176 countries and has revolutionized endpoint protection by being the first and only company to unify the three crucial elements of cybersecurity – next-generation anti-virus, endpoint detection and response (EDR), and 24/7 managed hunting services.

CrowdStrike’s platform is delivered via the cloud in a single lightweight sensor, enabling instantaneous real-time visibility into adversary activity on every endpoint device. Its endpoint protection platform, CrowdStrike Falcon, is the first true software-as-a-service (SaaS) platform and uses the patent-pending CrowdStrike Threat Graph to analyze and correlate billions of events in real time, providing complete protection and visibility across all endpoints in mere seconds. With a number of open APIs, the Falcon platform has become a critical component of organization’s enterprise security strategy.

CrowdStrike customers have access to CrowdStrike OverWatch, an elite force of renowned threat hunters, intrusion analysts and first responders who proactively hunt for threats on clients’ networks 24/7/365. This critical part of CrowdStrike Falcon’s value proposition amplifies clients’ internal security resources with the powerful support of its in-house security team to respond in real-time, anytime.

It also provides expertise for customers to continually leverage, improve and expand the capabilities of CrowdStrike Falcon.

CrowdStrike is driving major innovations around machine learning to scale the knowledge of skilled human analysts to large data sizes.
HIS TEAM FOILED A SECURITY THREAT THAT COULD HAVE COST HIS COMPANY MILLIONS.

HOW? HE’S NOT TELLING.

Splunk® solutions give security teams visibility across the entire infrastructure so they can quickly detect and contain threats to their organization. 85 of the Fortune 100 use Splunk software and cloud services to gain a competitive advantage and protect their business, but only a few of them will talk about it.

just ask What can you do with Splunk? Stop by the Splunk booth #N3421
Excellence Award
BEST SME SECURITY SOLUTION

WINNER
eSentire for eSentire Managed Detection and Response

eSentire is an industry leader, providing managed threat detection and response services to clients, keeping their high-risk assets safe from the complex and constantly evolving cyber-threats that traditional security defenses simply can’t detect. Combining people, process and proprietary technology, eSentire delivers an unmatched premium-level service that hunts, detects, remediates and communicates sophisticated cyberthreats in real-time, 24/7. Protecting more than $3.2 trillion in assets under management (AuM) and more than 1,500 sensors in 30 countries, eSentire is the award-winning choice for mid-market security decision-makers. eSentire has expanded operations beyond its Canadian headquarters, with sales offices and Security Operations Centers across North America and Europe (U.K. and Ireland). Over the last five years, its client base has more than doubled, with a 95 percent client retention rate.

eSentire Managed Detection and Response keeps mid-sized organizations safe from constantly evolving cyberattacks that traditional security defenses aren’t able to detect. Smarter than traditional technologies, eSentire MDR goes beyond intrusion prevention (IDS/IPS) and system information and event management (SIEM) – it leverages full-packet capture, signature-based threat intel, behavioral and reputational-based analytics, and attack-pattern algorithms to detect both known and unknown cyberthreats. It’s more effective because its 24/7 SOC analysts use powerful forensic tools to hunt, fully investigate and respond to real attacks before they can do harm to clients’ networks. Its award-winning service combines proprietary technology with a team of sophisticated security analysts, monitoring client networks 24/7 to hunt, defend and mitigate against known and unknown cyberthreats.

Finalists 2017
• eSentire for eSentire Managed Detection and Response
• DigiCert for CertCentral
• Netsurion for remote-managed security
• Versasec for vSEC:CMS 4.5
• Webroot for SecureAnywhere Business Endpoint Protection

Excellence Award
ROOKIE SECURITY COMPANY OF THE YEAR

WINNER
Contrast Security

Contrast customers continue to demonstrate strong interest and adoption for Contrast Runtime Application Self-Protection (RASP), which provides both up-sell and new customer acquisition opportunities.

Before Contrast Enterprise, these capabilities were only available in separate, siloed products from different vendors. When vendors partnered and integrated AppSec testing tools with attack protection products, the joint solutions were too complicated and woefully inaccurate to deliver on the vision.

Contrast is pushing the boundaries of what’s possible. Embedded in each of its teams is at least one engineer with a commanding grasp of the internals of the virtual machine or platform they’re in charge of protecting. Each team also has an app security expert. This makes for a unique organization. It has small, highly specialized teams that use complementary experience to accomplish shared goals without having a separate R&D team.
Global Learning Systems for Security Awareness Training Program

The overall GLS Security Awareness Training (SAT) Program includes a comprehensive suite of 40 targeted end-user courses and modules designed to educate and drive positive behavior change within an organization. Program course options include the following elements chosen based on client requirements: annual SAT courses in 25- and 40-minute versions; a large library of topic-based Best Practice Modules distributed monthly or quarterly for ongoing awareness, as well as a library of short animated videos to reinforce key best practices. Specialized courses are available for clients with more mature SA programs to targeted groups. These include Anti-Phishing Essentials Training and role-based courses to target IT security professionals including administrators, developers and executives. Personalized curriculum is now delivered and tracked online with automation, assessment, testing and reporting features. The result is that with on-going monitoring and reassessment, the tool improves user knowledge by delivering engaging programs that address knowledge gap areas.

GLS provides clients with a true end-to-end solution that can be tailored to the unique requirements of each user and client organization. Rather than just providing a standard “out of the box” or “turnkey” product package, clients choose GLS for its ability to provide a flexible, consultative approach, looking at the needs of their organization. Clients select GLS for its modular library with rich content design using scenario-based learning and gamification elements, as well as competitive pricing and robust tools to drive behavior change.

The quality and diversity of GLS programs are the differentiators, along with its focus on overall client satisfaction and measuring success using its products and services.

ISACA for Certified Information Systems Auditor (CISA)

ISACA, a global association serving 140,000 IT and cybersecurity professionals in more than 180 countries, provides leading guidance, training and research for members and nonmembers through conferences (in-person and virtual), webinars, a bimonthly journal, training courses, research publications, blogs and white papers. ISACA also offers a global network of 215 chapters in 92 countries, providing professionals local training, professional networking, certification review courses and opportunities for the exchange of global best practices. Members are provided opportunities to take on leadership roles, participate in the development of research publications and speak at global conferences. Additionally, ISACA created Cybersecurity Nexus (CSX) to help organizations develop skilled cyber workforces and to enable individuals to grow and advance their cyber careers.

CSX provides guidance, training, career development, education, research and credentials for cybersecurity professionals at every stage of their careers. Considered the gold standard of certifications for IS audit, control and assurance professionals, the CISA certification has been earned by more than 126,000 professionals since its inception in 1978. CISA differentiates itself from other offerings with its accreditation from the American National Standards Institute (ANSI) under the International Standard ANSI/ISO/IEC 17024 and its regular listing among the highest-paying certifications in Foote Partners IT Skills and Certification Pay Index. CISA also was listed among the highest-paying certifications in Global Knowledge’s 2016 IT Skills and Salary Survey. The exam’s quality is ensured through a rigorous process that includes a job practice analysis study and regular content reviews by independent committees.

ISACA for Certified Information Systems Auditor (CISA)
WINNER
City of Los Angeles

With four million residents, the city of Los Angeles (LA) is the second largest city in the U.S. It is also the largest cybertarget on the West Coast. The LA’s Information Technology Agency (ITA) manages the IT systems and network traffic for 40 departments with 35,000 full-time employees.

Timothy Lee, CISO of the city of Los Angeles, and his team, ITA Information Security Office (ISO), are charged with protecting LA’s critical infrastructure and high-value targets, including those that support the LA’s financials, transportation, utilities, water treatment plants, public safety and law enforcement. The ISO team is overseeing daily security operation activities and cybersecurity tools that are analyzing average 300 million security-related events and stopping an average of three million unauthorized access attempts daily.

The CISO and his team established a Cybersecurity Strategic Plan based on the NIST Cybersecurity Framework and successfully implemented the program that dramatically improves the LA’s security posture.

The team has successfully implemented the city’s first $1.8 million, state-of-the-art Integrated Security Operations Center (ISOC). The ISOC collects massive security data from all 40 departments to a single security analytics platform and provides real-time security posture dashboard to stakeholders for situational awareness (SA), and disseminates actionable threat intelligence. The project has received several awards.

Lee and his team work closely with officials across the key departments of LA (water and power, LA airport, the Port of Los Angeles and the IT Agency) to improve the city’s cybersecurity posture. Tim Lee chairs the governance body, Cyber Intrusion Command Center (CICC), to coordinate preparation and response across city departments.

WINNER
Tim Callahan, SVP, global chief security officer, Aflac

Tim Callahan has effectively developed and managed a strong IT security team largely because, on joining Aflac, he convinced executive management and the board of directors of the need to modernize the security program. He has since established an organization of more than 80 professionals, providing strategy and vision and empowering the team to build their programs. For example, Callahan leads the continuous development of methods and best practices for a leading-edge intelligence program that includes predictive analysis and dark web inspection. He also conducted an enterprise risk assessment and developed a security strategy built on risk particular to Aflac. He challenges his team daily to improve how they gather and analyze both strategic and tactical intelligence, reminding them that it is an iterative process. It’s important that they build a protocol to judge credibility and applicability as rapidly as possible and then act on the intel.

Callahan has gained the support of corporate leaders by keeping Aflac’s board updated about the company’s security metrics and progress. He frequently attends board meetings and provides detailed assessments of which IT systems the company monitors in real time, as well as efforts to assess and defend against spyware and malware. Callahan benchmarks Aflac’s security spending against insurance industry norms and updates the board about attack statistics, including spyware, malware and security policy violations by Aflac employees.

Aflac has adopted the National Institute of Standards and Technology Cybersecurity Framework from the U.S. Department of Commerce, and Callahan presents “maturity reports” that show how Aflac compares to the NIST guidelines.

Finalists 2017
- City of Los Angeles
- Fairfax County
- MasterCard
- Pasona NA

Finalists 2017
- Connie Berrera, CISO, Jackson Health System
- Tim Callahan, SVP, global chief security officer, Aflac
- Emily Heath, global CISO, AECOM
- Pritesh Parekh, VP, chief security officer, Zuora
- Myrna Soto, SVP, global CISO, Comcast Cable
This year, we recognize the National Cyber Security Alliance (NCSA) for its efforts in promoting cybersecurity awareness – not just for large enterprises but for home users as well.

The nonprofit was founded in 2001 as a public-private partnership, working with the Department of Homeland Security (DHS) and a range of partners to educate and empower digital citizens to more safely use the internet and the burgeoning universe of mobile devices.

The group started National Cyber Security Awareness Month and the government’s Stop. Think. Connect. campaign to spread the message of cyber safety. And, every January 28, it celebrates Data Privacy Day. This past January, it hosted a day-long event streamed live from Twitter’s headquarters in San Francisco featuring discussions focusing on privacy issues. This annual event brings together industry, government and nonprofit collaborators to spread knowledge about better protecting personal information.

The theme for 2017’s Data Privacy Day centered on “Respecting Privacy, Safeguarding Data and Enabling Trust.” As always, the event intends to help consumers learn more about managing their privacy and protecting their personal information, as well as encouraging businesses to be more transparent about how they collect and use data, according to the site.

“With so many of our day-to-day activities carried out online, Data Privacy Day reminds everyone to manage their digital lives with concrete, simple and actionable steps,” Michael Kaiser, executive director of NCSA, said in a statement. “We can only build a safer, more trusted internet if everyone works in collaboration to make respecting and protecting personal information a priority.”

Kaiser and the NCSA work to unite government, corporate, nonprofit and academic organizations to promote the importance of cybersecurity. Since coming on as director of the alliance in September 2008, Kaiser has strengthened partnerships with the U.S. Department of Homeland Security and other federal government agencies and fostered new ones with state and local governments. In 2009, Kaiser was named one of SC Magazine’s information security luminaries. He is a tireless advocate for cybersecurity, appearing on numerous panels and at trade shows.

Early in 2016, the NCSA instituted a program to promote greater public understanding of multifactor authentication, expanding its education efforts under the STOP. THINK. CONNECT. umbrella to support a broader effort to increase public awareness of the individual’s role in cybersecurity.

To bring awareness of cybersecurity and privacy issues directly to local communities, NCSA’s education project partnered with information technology and training companies Logical Operations, New Horizons and CompTIA with a “Get Two Steps Ahead: Protect Your Digital Life” tour to more than 15 cities nationwide. At these presentations, attendees received hands-on training in multifactor authentication and gained a sense of how vital it is to their own online safety.

And Kaiser’s diligence is increasingly necessary as the complexity of our tethered activity online only increases. “IoT is really the Internet of Me,” he said. “As we continue to acquire devices and apps to make our lives more convenient and efficient, we need to be aware that the cadence of our lives is being digitally captured. Data Privacy Day is a time for all digital citizens to carefully consider the data they continuously generate about themselves and others and take steps to protect their personal information and manage their privacy.”

While he acknowledges that awareness around cybersecurity and privacy issues has improved, there is still a need for more education around how our data is collected, managed and used, he said. “Personal information has value – just like money. It’s critically important for everyone to continue to learn about the data use practices of the companies, websites and devices with which they interact and consider how they can better manage their digital lives.”
DEFEATING ADVANCED THREATS TAKES MORE THAN JUST PREVENTION.

Protecting your organization’s user endpoints and critical servers requires much more than basic threat prevention. Legacy antivirus cannot keep up with the growing onslaught of sophisticated new malware, and even next-gen AV solutions still focus only on file-based malware prevention, leaving you with no other protective measures against other attacks.

SentinelOne’s Endpoint Protection Platform (EPP) protects endpoints against every threat vector from advanced malware, to exploits and stealthy insider threats. It pairs signatureless static prevention with state-of-the-art behavioral detection, and seamlessly incorporates automated policy-driven response and full-context forensics.

**The result?** Unified, next-generation endpoint protection that addresses the entire threat lifecycle.

**SentinelOne EPP Benefits**

- Protects endpoints and servers running Windows, MacOS, and Linux
- Certified AV replacement for Windows and MacOS endpoints
- Easily deployed, scaled, and managed (cloud-based or on-premise)
- Delivers up to 5x better Total Cost of Ownership than a multi-solution approach to NGEP

For more information about SentinelOne and the future of endpoint protection, please visit: [www.sentinelone.com/contact](http://www.sentinelone.com/contact)

© 2017 SentinelOne, Inc. All rights reserved.