SC 2019 awards

Honored in the U.S.

March 5, 2019 • San Francisco

#scawards

SC celebrates 30 years



This year is special for SC Media. We commemorate 30 years as part of the cybersecurity, if you prefer, infosec community.

So, as part of our annual SC Awards celebration, not only are we calling out the best and brightest people, organizations and solutions from this last year, we also launched an ancillary program to pay tribute to those individuals and organizations that have contributed to the wider community over these last 30 years.

While we relied on our esteemed panel of judges to help choose our finalists and winners for our traditional SC Awards program, members of our editorial team and my 2019 SC Awards co-chairs Chris Painter and VJ Viswanathan helped pick the winners for the 30th Anniversary Award categories. We are indebted to all.

As we looked back on the headlines that comprised these last 30 years the old adage had a ring of truth to it: The more things change, the more they stay the same. That's because peppered throughout these stories were mentions of mobile security concerns, cyberwarfare, e-commerce vulnerabilities, password woes, security awareness training, identity and access management issues and supply chain concerns. And, now, in 2019 we're still discussing the same worries.

However, the scale and size of these problems today are astronomically different. The vectors of attack continue to grow – from seemingly countless IoT risks, to the infiltration of electoral systems and our critical infrastructure. AI and machine learning, today's catch phrases, also have made strides, and not only can enable the automation of security or other functions for businesses, but may also end up enabling cybercriminals and their activity.

Keeping up with this changing landscape is not easy and yet, security leaders like you have made innumerable strides to safeguard organizations and critical data, enable your businesses and help profitability. This progress has set the pace in which we now find ourselves. And while it's never easy to keep up, there are moments of victory.

These victories – the ones that bolster resiliency and security strategies, thwart a data breach, the moments that garner true, palpable support from your CEO, – are what we celebrate with our annual SC Awards. We pay tribute to these victories and to all of you who make them happen. Cheers to you all… and to 30 more years!

– Illena Armstrong, VP, editorial, SC Media

SC 2019 awards

Honored in the U.S.

Contents

Judges 4
Sponsors 6
Welcome from the co-chairs 8

Trust Awards

Best Authentication Technology 8
Best Business Continuity/Disaster Recovery Solution 9
Best Cloud Computing Security Solution 9
Best Computer Forensic Solution 10
Best Data Leakage Prevention (DLP) Solution 10
Best Database Security 11
Best Deception Technology 11
Best Email Security Solution 12
Best Identity Management Solution 12
Best Managed Security Service 13
Best Mobile Security Solution 13
Best NAC Solution 14
Best Risk/Policy Management Solution 14
Best SCADA Security Solution 15
Best SIEM Solution 15
Best Threat Detection Technology 16
Best Threat Intelligence Technology 16
Best UTM Security Solution 17
Best Vulnerability Management Solution 17
Best Web Application Solution 18

Excellence Awards

Best Customer Service 18
Best Emerging Technology 19
Best Enterprise Security Solution 19
Best Regulatory Compliance Solution 20
Best Security Company 20
Best SME Security Solution 22
Rookie Security Company of the Year 22

Professional Awards

Best Cybersecurity Higher Education Program 23
Cybersecurity Student of the Year 23
Best IT Security-related Training Program 24
Best Professional Certification Program 24
Best Security Team 26
CSO of the Year 26
Editor's Choice Award 28

EDITORIAL
VP, EDITORIAL Illena Armstrong
EXECUTIVE EDITOR Teri Robinson
ONLINE EDITOR Doug Olenick
SENIOR REPORTER Bradley Barth
CONTENT COORDINATOR Robert Abel

SC AWARDS 2019
VP, EVENTS Adele Durham
EVENTS MANAGER Anna Naumoski
VIRTUAL EVENTS DIRECTOR Jourdan Davis

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
PRODUCTION MANAGER Brian Wask

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

U.S. SALES
VP, GROUP PUBLISHER David Steifman (646) 638-6008
VP, SALES Matthew Allington (707) 651-9367
DIRECTOR, STRATEGIC ACCOUNTS Roz Burke (774) 208-3652
DIRECTOR, STRATEGIC ACOUNTS Michael Greenhut (845)-499-9774
DIRECTOR, STRATEGIC ACCOUNTS Robyn Armao (914) 263-4178
BRAND & MARKETING MANAGER Kelsey Schoepfer (646) 638-6137
MARKETING SPECIALIST Alexa Fletcher
DIRECTOR OF LEAD GENERATION AND DATA STRATEGY Danielle Azzara
CUSTOM PROJECTS COORDINATOR Samantha Lubey (646) 638-6094

Aflac®

Congratulates

Tim Callahan

for being recognized as a recipient of the

2019 SC Magazine 30th Anniversary Awards

Information Security Executives of the Last 30 Years



Z190296

Aflac herein means American Family Life Assurance Company of Columbus and American Family Life Assurance Company of New York | AFLAC HQ | 1932 Wynnton Road | Columbus, GA 31999.

EXP 3/20

The Judges

Big thanks to our 2019 Jurors!

CO-CHAIR
Chris Painter,
Global Commission on the Stability of Cyberspace

CO-CHAIR
VJ Viswanathan
Keurig

Roota Almeida,
Delta Dental

Ron Baklarz

Daniel Basile,
Texas A&M University System

Todd Bell,
Intersec Worldwide

Bob Berbeco,
Adult & Child

Benjamin Bergersen,
U.S. Trade and Development Agency

Jon Bowker,
Ingo Money

Joshua Bregler,
Beyond Mission Critical Systems

Miki Calero,
Urbis Global LLC

Todd Caron,
Align Credit Union

John Christly,
WHOA Networks

Steve Cobb,
One Source Communications

Leo Cuellar,
Taos

Alex Cunningham,
Commonwealth Financial Network

William Dailey,
Transaction Data Systems

Shomiron Das Gupta,
DNIF

Stephen Davis,
Macmillan

Laszlo Dellei,
UNIQA Insurance Hungary

Rick Doten,
Crumpton Group

Nikesh Dubey,
AGC Networks

Paul Dumbleton,
Gordon Food Service

Steven Ferguson,
Technical College System of Georgia

Matt Franz,
Clark State Community College

Pamela Fusco,
CBG

Ajit Gaddam,
Visa

Terry Gold,
D6 Research

Tyrone Grandison,
The Data-Driven Institute

Todd Grober,
Ernst & Young

Dheeraj Gurugubelli,
Deloitte and Touche LLP

Vincent Hamm,
Aim High!, Inc.

Mansur Hasib,
University of Maryland University College

John Johnson,
Aligned Security

Peder Jungck,
BAE Systems

Ashutosh Kapsé,
IOOF Holdings

Hilik Kotler,
FICO

Curt Kwak,
Proliance Surgeons

Chris Lambrou,
Metro MLS

Cedric Leighton,
Cedric Leighton Associates and CYFORIX

Chris Letterman,
Wostmann & Associates

Gary Long,
Long Professional Services

Ryan Loy,
EBSCO

Aditya Malhotra,
Point72 Asset Management

Richard Marshall,
Cinturion Group

Sean McElroy,
Lumin Digital

Zachery Mitcham,
North Carolina Central University

Travis Paakki,
Portland Public Schools

Mitchell Parker,
Indiana University Health

David Poe,
United Way of Greater St. Louis

Robecca Quammen,
HealthITq

Bhuvaneswari Ramkumar,
GE-Digital

Todd Redfoot,
Go Daddy

Philip Rizzo,
E-data Law Group

Sandi Roddy,
JHU APL

Vincent Romney,
Younique Products

Marcus Sachs,
Pattern Computer

Randolph Sanovic,
RNS Consulting

Steve Santorelli,
Team Cymru

Stephen Sparkes,
Bank of America

Rick Stanbridge,
Marco's Franchising

Bobbie Stempley,
Carnegie Mellon University

Dona Stines,
Rampart Supply

Priscilla Tate,
TechForum

Dennis Thibodeaux,
New Horizons Computer Learning Centers

Richard Timbol,
Davis Polk

Krishna Vedula,
365 Retail Markets

Lauren Zink,
AmTrust Financial


BURNT BY A
SIEM
Try a SOC-as-a-Service
Before You Crash and Burn
Learn more at
www.arcticwolf.com/burnt_by_a_siem
ARCTIC
WOLF

The Sponsors

SC Media thanks all sponsors for their generous support of the SC Awards 2019. 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, helping provide protection to more than 50 million people in Japan and the U.S., giving policyholders the opportunity to focus on recovery, not financial stress. Through its trailblazing One Day PaySM initiative in the U.S., Aflac can process, approve and electronically send funds to claimants in just one business day. For 13 consecutive years, Aflac has been recognized by Ethisphere as one of the World's Most Ethical Companies, and in 2019, Fortune included Aflac on its list of World's Most Admired Companies for the 18th time. Find out more at Aflac.com.

Arctic Wolf Networks

Arctic Wolf Networks delivers the industry-leading security operations center (SOC)-as-a-service that redefines the economics of cybersecurity. The AWN CyberSOC™ service is anchored by Concierge Security™ teams who provide custom threat hunting, alerting, and reporting. Arctic Wolf's purpose-built, cloud-based service offers 24x7 monitoring, vulnerability assessment, threat detection, and response. For more information about Arctic Wolf, visit https://arcticwolf.com.

AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning – helping to enable our customers around the globe to anticipate and act on threats to protect their business.

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 and are delivered in appliance, virtual appliance, cloud and hybrid deployment configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data protection. For additional information, please visit barracuda.com.

Digital Defense, Inc.

Serving clients across numerous industries, Digital Defense's innovative and leading-edge technology helps organizations safeguard sensitive data and eases the burdens associated with information security. Frontline.Cloud, the original Security SaaS platform, delivers unparalleled accuracy and efficiencies through multiple systems including Frontline Active Threat Sweep™ (Frontline ATS™), Frontline Vulnerability Manager (Frontline VM™), Frontline Web Application Scanning (Frontline WAS™) and Frontline Pen Test™, while SecurED®, the company's security awareness training, promotes employees' security-minded behavior. The Digital Defense Frontline suite of products, underpinned by patented technology and complemented with superior service and support, are highly-regarded by industry experts, as illustrated by the company's designation as #10 ranking in The Saas Report's Top 25 CyberSecurity Companies of 2018, recipient of Frost & Sullivan's 2018 Global Vulnerability Management Customer Value Leadership Award, #10 ranking in Black Book Market Research's list of Compliance & Risk Management Solutions, and inclusion in CRN's 2018 MSP 500. Contact Digital Defense at 888-273-1412; visit www.digitaldefense.com, our blog, LinkedIn, or follow @Digital_Defense on Twitter.

Kimberly-Clark

Kimberly-Clark (NYSE: KMB) and its trusted brands are an indispensable part of life for people in more than 175 countries. Fueled by ingenuity, creativity, and an understanding of people's most essential needs, we create products that help individuals experience more of what's important to them. Our portfolio of brands include Huggies, Kleenex, Scott, Kotex, Cottonelle, Poise, Depend, Andrex, Pull-Ups, GoodNites, Intimus, Neve, Plenitud, Viva and WypAll.

Recorded Future

Recorded Future delivers the only complete threat intelligence solution powered by patented machine learning to lower risk. We empower organizations to reveal unknown threats before they impact business, and enable teams to respond to alerts 10 times faster. To supercharge the efforts of security teams, our technology automatically collects and analyzes intelligence from technical, open web, and dark web sources and aggregates customer-proprietary data. Recorded Future delivers more context than threat feeds, updates in real time so intelligence stays relevant, and centralizes information ready for human analysis, collaboration, and integration with security technologies. 91 percent of the Fortune 100 use Recorded Future.

Cisco Talos Intelligence Group

Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts and engineers. These teams are supported by unrivaled telemetry and sophisticated systems to create accurate, rapid and actionable threat intelligence for Cisco customers, products and services. Talos defends Cisco customers against known and emerging threats, discovers new vulnerabilities in common software, and interdicts threats in the wild before they can further harm the internet at large. Talos maintains the official rule sets of Snort.org, ClamAV, and SpamCop, in addition to releasing many open-source research and analysis tools.

Zix

Zix is a leader in email security and trusted by more than 21,000 customers, including the nation's most influential institutions in healthcare, finance and government. Zix delivers superior, easy-to-use solutions and exceptional support for email encryption and data loss prevention, advanced threat protection, unified archiving and bring your own device (BYOD) mobile security. Focusing on the protection of business communication, Zix enables its customers to confidently defend against the latest email attacks, better secure data in email and meet compliance needs. For more information, please visit www.zixcorp.com.


AT&T Business
AT&T Business + AlienVault
join forces to create the new
AT&T Cybersecurity
To learn more, visit: www.alienvault.com/joiningforces

Welcome from the co-chairmen

I've been involved in cybersecurity and cyber policy for over 25 years – in the public and private sectors, as well as, academia. But, as long as my tenure has been, SC Magazine has been around even longer.

For 30 years SC has been an industry staple and the go-to source for information and advice for this once fledgling industry. Back when SC started, computers and networks were of limited importance and security was seen as an afterthought. Today, governments are starting to realize that cybersecurity is a core part of national and economic security and C-Suite executives are beginning to understand that cybersecurity is not just a cost center, but vital to their bottom line and future competitiveness.

Of course, there are still many challenges ahead, but we are making real progress. SC Magazine has not only witnessed and aided that progress, but has also advanced and evolved. Its award program has helped recognize leaders and innovation and served to elevate the entire industry. SC continues to be a vital player in this ever-expanding field. Here's to 30 more years of insightful news, analysis and advice.

– Christopher Painter
Willam Perry Fellow
Center for International Security
and Cooperation, Stanford University



SC Media has a long-standing tradition of evolving to meet market needs with a penchant for innovation and disruptive changes that deliver immense value to security leaders, product brands and partners. The value created is the result of 30 years of focused leadership, engagement and guidance in cybersecurity, risk management and compliance markets. This active engagement between editorial and industry experts has created a unique platform that delivers a one of a kind differentiating experience.

The mission of SC Awards is to honor and celebrate the achievements of the cybersecurity brands and professionals striving to safeguard businesses, their customers, and critical data.

Sixty-eight jurors and co-chairs partnered actively over the past few months to carefully evaluate the more than 500 entries. Selecting the 2019 SC Awards finalist and the winners was a collaborative effort and it is worth reflecting upon the diligence and creativity invested by the team members that made up the collective competing brands. So please joing us in recognizing excellence in the cybersecurity industry and to celebrate 30 brilliant years of SC Media.

– VJ Viswanathan,
CSO, Keurig Dr Pepper



Trust Award

BEST AUTHENTICATION TECHNOLOGY

WINNER

RSA Security for RSA SecurID Access

There's only one "you," but at least there's plenty of ways to prove you're you.

That's especially true when using RSA SecurID Access, a smart authentication platform that offers a host of user verification options, including mobile push notifications, one-time passwords, fingerprint and facial biometrics, SMS messages, voice recognition, FIDO tokens and hardware and software tokens.

Whenever a user requests access to sensitive data or systems, SecurID Access factors in variables such as user profile, threat risk and business impact to contextually generate a confidence score. If confidence is high, the user quickly and efficiently gains access, with minimal friction. But if the access request is determined to be a risky proposition, then the solution may ask for more explicit forms of authentication.

The SecureID Access data model is tuned to reduce the need for additional authentication by as much as 90 percent, but security admins can adjust assurance level settings up or down as desired, all from a centralized management console.

The solution can be applied toward a huge range of use cases involving cloud- and web-based systems, legacy applications, next-generation firewalls, privileged access management systems, managed workspaces and more from over 500 technology partners. User organizations can quickly onboard new apps by using wizard-based connectors for leading authentication protocols or by reusing preexisting integrations executed by the company's RSA Ready technology partner program.

RSA offers companies the option of installing SecureID Access as a virtual appliance to lower TCO, or as a cloud offering for which updates and changes are seamless. Adding to SecureID Access' convenience is a self-service enrollment feature that reduces administrative and support costs.

Finalists 2019

- Duo Security, Duo Security
- Okta, Adaptive Multi-Factor Authentication
- RSA Security, RSA SecurID® Access
- SecureAuth, SecureAuth IdP
- WatchGuard Technologies, WatchGuard AuthPoint



Trust Award

BEST BUSINESS CONTINUITY/ DISASTER RECOVERY SOLUTION

WINNER

Druva for Druva Cloud Platform

Disasters: They're not always preventable or predictable. Sometimes the best that can be done is minimize the damage. To that end, the Druva Cloud Platform (DCP) ensures that data doesn't have to be a casualty.

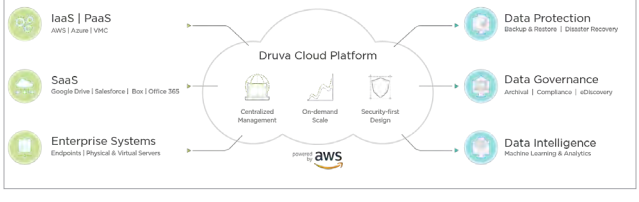
Druva provides comprehensive and cost-effective cloud-based disaster recovery protection, offering its customers agentless VM backups at the ready, to enable recovery within minutes of an incident.

But it's much more than that. The solution presents a unified control plane for data management services across the enterprise, including data found on endpoint servers, in cloud applications and in cloud workloads. Such visibility lowers the cost of data protection by over 60 percent, whether the data resides on physical or virtual servers, or is managed in an SaaS, PaaS or IaaS environment.

Implemented natively on Amazon Web Services, DCP provides streamlined storage management and elasticity, all while automating data's life cycle management. Even as it safeguards the data, DCP optimizes customer environments through global data deduplication and the consolidation of storage and DR products.

Additionally, data centers around the globe provide 99.99999 percent data durability and infinite scale, while enabling alignment with regional data residency requirements.

One city that knows how disasters can devastate local businesses is New Orleans. The Port of New Orleans has experienced major time savings since selecting Druva for data backups and restores. Backups that once took four to eight hours per system now take 30 minutes or less. Users can now restore files on their own, with only five minutes of training, while the number of calls to the Port's IT department has dropped by 60 to 70 percent.



Finalists 2019

- Cloud Daddy, Cloud Daddy Secure Backup
- Druva, Druva Cloud Platform
- Hedvig, Hedvig Distributed Storage Platform 3.8
- Quest Software, NetVault Backup 12.1
- RackTop Systems, RackTop Systems

Trust Award

BEST CLOUD COMPUTING SECURITY SOLUTION

WINNER

McAfee for McAfee MVISION Cloud

Who says high visibility isn't possible in heavy cloud environment? Pilots, maybe. But not security professionals, especially those familiar with MVISION Cloud.

McAfee's innovative cloud access security broker (CASB) solution allows security professionals to set consistent data and threat protection policies across SaaS, IaaS, PaaS, private cloud, hybrid cloud and multi-cloud environments – all from a centralized, single-pane console.

MVISION Cloud is capable of tracking more than 50 security attributes and over 250 sub-attributes for 25,000+ cloud services. According to McAfee's nomination, it normally takes an IT department roughly 17 days to vet a cloud service, but MVISION can accomplish this task in mere minutes. Consequently, user organizations are able to reduce the number of man-hours allocated toward cloud governance and adoption by as much as 80 percent.

With superior visibility into their cloud usage patterns, customers can realize additional cost savings by identifying and consolidating redundant services. Knowing exactly how many licenses they truly need based on the number of employees and developers who actually use them allows them to negotiate better volume deals with their cloud vendors.

Part of the MVISION portfolio, MVISION Cloud works in tandem with the data loss prevention solution McAfee DLP to create a unified data protection experience across the customer's entire corporate network. This provides users with total control over both physical and cloud-based assets, including endpoints, servers and virtual servers, data, apps and services, network-traffic flow and container workloads.



Finalists 2019

- Attivo Networks, ThreatDefend™ Deception and Response Plat-form
- Bitglass, Bitglass Cloud Security
- CipherCloud, CipherCloud CASB+ Platform
- Cisco, Umbrella Secure Internet Gateway
- Dome9 Security, Dome9 Arc platform
- McAfee, McAfee MVISION Cloud
- Proofpoint, Proofpoint Cloud App Security

Trust Award

BEST COMPUTER FORENSIC SOLUTION

WINNER

OpenText for EnCase Forensic, EnCase Endpoint Investigator and EnCase Mobile Investigator

When OpenText acquired Guidance Software in September 2017, it inherited not just the latter company's EnCase product line, but also a seven-year winning streak in SC's Computer Forensic Solution category. After extending that run to eight last year, OpenText now makes it nine consecutive victories, triumphing again with a trio of solutions: EnCase Forensic, EnCase Endpoint Investigator and EnCase Mobile Investigator.

Collectively, these investigation tools benefit government agencies and law enforcement officers as they gather forensic evidence in criminal probes, while helping corporate investigators look into HR issues, compliance violations, regulatory inquiries and IP theft.

In 2018, OpenText extended its reach into the IoT space by introducing a Raspberry Pi agent for its Mobile Investigator solution, which lets organizations view, analyze and report on critical mobile evidence.

EnCase Forensic, meanwhile, continues to allow investigators to efficiently conduct digital analysis on any operating system and parse virtually any file type. And EnCase Endpoint Investigator provides seamless and discreet remote access to laptops, desktops and servers, without disturbing day-to-day end users. Its user interface supports 14 different languages while reducing human error and encouraging collaboration.

User organizations ultimately increase productivity and reduce staffing fees and outsourcing costs by automating the laborious investigation processes into a few simple steps, even as they collect evidence from vast datasets. In fact, customers often surpass a 100 percent return on investment upon completing their first few investigations.

Finalists 2019

- AccessData, Forensic Toolkit (FTK)
- D3 Security, D3 Automated Incident Response and Case Management Solution
- Endace, 9200 Series EndaceProbe Analytics Platform
- OpenText, EnCase® Forensic, EnCase Endpoint Investigator & EnCase Mobile Investigator
- PacketSled, PacketSled



Trust Award

BEST DATA LEAKAGE PREVENTION (DLP) SOLUTION

WINNER

Forcepoint for Dynamic Data Protection

When it comes to which employees pose the greatest risk of data exfiltration, Forcepoint knows the score.

As in risk score. Forcepoint's machine-learning-based Dynamic Data Protection solution dynamically assesses each worker's behavioral risk score, continuously adjusting it up or down with each action he or she initiates on corporate or unmanaged networks, across multiple machines and accounts.

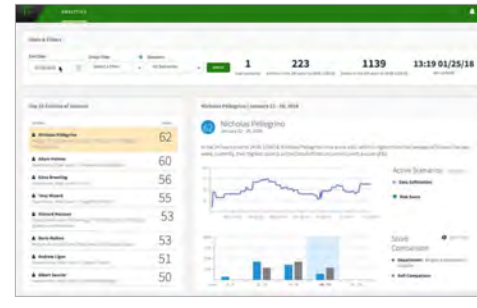
Using human-centric behavior analytics, the solution establishes each end user's baseline of "normal" behavior. As it identifies potentially unsafe activity, the risk-adaptive technology responds, in automated fashion, by applying various security countermeasures.

The severity of the response is dictated by the perceived risk. Under various circumstances, the solution might allow and monitor a user's access to sensitive data, allow access but encrypt downloads, or completely block access. Consequently, employees labelled as high-risk might find that they are prevented from emailing sensitive information or moving or copying materials to a removable drive.

Bottom line: with Forcepoint, rule enforcement can be user- and task-specific, rather than applied broadly in a one-size-fits-all manner.

The solution's dynamic scoring mechanism offers a significant advantage over traditional static risk assessments that can quickly become outdated, while the automated nature of the product helps relieve the burden on security analysts who would otherwise be overwhelmed sifting through endless red flags and security alerts. This frees up their time to instead prioritize high-value projects and investigations.

Of course, the biggest benefit of all may be the prevention of data loss by stopping a potentially damaging action in its tracks.



Finalists 2019

- Digital Guardian, Digital Guardian Data Protection Platform
- Fidelis Cybersecurity, Fidelis Network
- Forcepoint, Dynamic Data Protection
- Symantec, Symantec Data Loss Prevention
- VMware, VMware Workspace ONE

Trust Award

BEST DATABASE SECURITY

WINNER

Imperva for Imperva FlexProtect for Database (formerly SecureSphere)

A challenge CIOs often face when asking management to invest in cybersecurity is finding demonstrable ROI or cost savings. So when you actually can justify an expenditure with hard financial data, that's a big win.

Imperva may have done just that: A Total Economic Impact study it recently commissioned found that switching from a legacy database security solution to Imperva FlexProtect for Database saves customers more than $3 million in present value over a three-year period.

A large portion of that $3 million total – $2.4 million – is saved by avoiding maintenance, support and upgrade costs typically associated with legacy software solutions that are no longer needed. And roughly $884,000 in savings is achieved through improving the database security staff's productivity through automation and simplified administration.

FlexProtect for Database is a centralized platform that enables collaboration between an organization's IT, security and compliance teams to ensure data protection and oversight across all on-premises database servers, big data environments and cloud database services. Capable of processing and analyzing billions of database events, the solution automates the discovery and classification of sensitive data, the assessment of database vulnerabilities, and the identification of suspicious data – all to stop threats in real time.

Using machine learning and behavior analytics, the solution also monitors which users access what data and what they are doing with it, flagging anomalous activity and policy violations. Customers can remove monitoring and reporting workloads off their database server, so it can be fully optimized for performance and availability. Such advantages improved cost of ownership at one unnamed computer manufacturer by 70 percent.



Finalists 2019

- Baffle, Baffle Advanced Data Protection Service
- Imperva, Imperva FlexProtect for Database (formerly SecureSphere)
- Netwrix Corporation, Netwrix Auditor
- Oracle, Oracle Database Security

Trust Award

BEST DECEPTION TECHNOLOGY

WINNER

Fidelis Cybersecurity for Fidelis Deception

Think of it like the good guy's version of phishing.

An organization adorns its network with a series of alluring decoy targets. Unwanted intruders who pursue these fake assets play right into the so-called victim's hands. Little do they know security professionals have already been alerted, and their activity is now being silently monitored and controlled.

It's hard to find a solution that sets a better trap than Fidelis Deception from Fidelis Cybersecurity, with its rich automation offerings that take the burden off of the human workforce while also allowing for ample scaling.

Available as an on-premise, cloud-based or hosted solution, Fidelis Deception works by automating the discovery of the user organization's environment and generating profiles of the most important assets, including even legacy systems, "shadow IT" systems and enterprise IoT devices.

It then deploys decoys and breadcrumbs to draw out any attackers who may have successfully breached the network, as well as insider threats and malwares. The subscription-based solution then tempts them with a variety of lures including fake data, file systems and admin accounts.

Decoys frequently change as the solution institutes occasional freshness cycles while also adapting to ongoing network environment changes.

Fidelis says its high level of automation enables deception layers to be managed and monitored in less than one hour per day by a tier-1 security analyst, with minimal false alarms. Fidelis Deception also offers superior network traffic visibility at sensor speeds of 10 Gbps, with the patented ability to discern the difference between human- and machine-based activity.



Finalists 2019

- Acalvio Technologies, ShadowPlex Cloud
- Attivo Networks, ThreatDefend™ Deception and Response Platform
- Fidelis Cybersecurity, Fidelis Deception
- Illusive Networks, Deception Management System
- TrapX Security, DeceptionGrid

Trust Award

BEST EMAIL SECURITY SOLUTION

WINNER

FireEye for FireEye Email Security

Email remains a favorite attack vector for distributing malware. Case in point: a 2018 FireEye report revealed that 46 percent of all ransomware attacks are delivered via email.

But as malicious code detection improves, some bad actors have shifted to malware-less scams like credentials phishing or Business Email Compromise.

FireEye Email Security distinguishes itself by countering both breeds of threats. It not only blocks attachments weaponized with malware, but it also seeks and destroys fraudulent wire transfer requests, URL links to credential phishing sites, and other social engineering and impersonation techniques. Whatever the malicious tactic is, FireEye is quick to identify it and quash it by leveraging first-hand intel on attacks and adversaries.

Aided by its 2017 acquisition of The Email Laundry, FireEye has built a collection of proprietary URL defense and attachment detonation technologies, as well as threat intelligence, machine learning and deep relationship analysis capabilities, to help clients identify true positive alerts in just four minutes.

FireEye Email Security's high detection efficacy and low false positive rate minimizes operational costs. And its ability to spot threats early minimizes potential damage from incidents.

It's proving to be an especially strong tool for government organizations migrating email management to the cloud. In 2017, FireEye became the first email security vendor to be authorized for government use for advanced threat protection by the Federal Risk and Authorization Management Program.

Commercial industries also benefit. Ben Cabrera, network supervisor at grocery chain Stater Bros. Markets, says the solution performs the workload equivalent of 1.5 employees who'd otherwise be required to manually track down security incidents. "We approximate this number to be $225,000 per annum in hard ROI," says Cabrera.



Finalists 2019

- Agari, Agari Email Trust Cloud™
- Cisco Systems, Cisco Email Security
- FireEye, FireEye Email Security
- Glasswall Solutions, Glasswall FileTrust ATP for Email
- Proofpoint, Proofpoint Email Protection

Trust Award

BEST IDENTITY MANAGEMENT SOLUTION

WINNER

Ping Identity for Ping Identity Platform

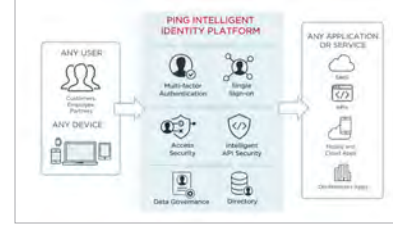
When it comes to identity and access management, the Ping Identity Platform is nothing if not thorough. From authentication to federation to authorization to data governance, Ping covers IAM from all angles, helping organizations large and small control access to cloud and on-premises applications from a single management point.

Built on open standards, Ping Identity protects more than 3 billion identities, providing users with powerful tools for password management, single sign-on and multi-factor authentication. Ping's simplified IAM experience speeds up productivity, while introducing efficiencies to the supply chain and customer transactions. Moreover, its partnership with top technology providers like Microsoft and Google allow it to facilitate access to a host of enterprise applications and data.

Debuting in 2018, the platform's newest addition, PingIntelligence for APIs, is an AI-driven solution that inspects API traffic activity, seeking out suspicious behavior that could indicate unauthorized hackers probing for vulnerabilities.

Ping holds a number of key advantages over typical legacy solutions, including rapid deployment and integration, which takes mere hours or days versus weeks or months. One customer, an unnamed U.S. telecom firm, saw an 80 percent reduction in its infrastructure footprint after switching from a legacy product to Ping, while also experiencing a two-fold boost in performance.

The financial software company Intuit implemented Ping's SSO solution, PingFederate, to ensure that its roughly 30,000 enterprise-wise identities could each use a single set of credentials to obtain one-click access to various applications. Ping's automated integration of new applications reduced Intuit's period of onboarding from one week to one day.



Finalists 2019

- CyberArk, CyberArk Privileged Access Security Solution
- Gemalto, SafeNet Trusted Access
- Okta, Okta Identity Cloud
- Ping Identity, Ping Identity Platform
- SailPoint, SailPoint's Open Identity Platform

Trust Award

BEST MANAGED SECURITY SERVICE

WINNER

Trustwave for Trustwave Managed Security Services

Trustwave Managed Security Services' elite team of 250 ethical hackers isn't just protecting some of the world's largest enterprises and government agencies. It's actually reimagining ways that entire industries can protect their assets.

In September 2017, Trustwave and its partner Inmarsat introduced an innovative way to introduce MSS to the maritime industry, delivering unified threat management services by way of satellite to commercial shipping and passenger vessels.

This is but one example of how Trustwave acts as a cyber "equalizer" for companies that otherwise lack the resources to defend themselves.

According to a model developed by Trustwave, a mid-size company managing its own SIEM deployment will spend more than $680,000 on hardware and personnel in year one alone, compared to just under $200,000 over the same time period if Trustwave MSS manages SIEM operations.

Run by Trustwave SpiderLabs, Trustwave MSS follows a tech-agnostic approach as it customizes its services based on clients' unique environments, technology investments and personnel skillsets.

Trustwave MSS also delivers actionable threat intelligence sourced from a global network of SOCs anchored by a central fusion center, as well as from a database that incorporates findings from research, pen testing and incident response efforts.

When a suspected breach occurs, Trustwave's DFIR (digital forensics, incident response) capabilities shorten the time to launch forensic investigations from days to seconds.

Each Trustwave MSS expert is assigned a finite number of customers within specific industries. This lets them develop specialized knowledge that helps them optimize a proper threat response such as blocking, containment or even eradicating the threat right down to the specific endpoint.



Finalists 2019

- Akamai Technologies, Prolexic DDoS Solutions
- Arctic Wolf Networks, AWN CyberSOC
- Digital Guardian, Digital Guardian's Managed Security Program (MSP)
- Proficio, Proficio
- Trustwave, Trustwave Managed Security Services

Trust Award

BEST MOBILE SECURITY SOLUTION

WINNER

VMware for VMware Workspace ONE

The ubiquity of mobile devices has turned just about any location into a potential workspace – from traditional offices to homes to vehicles and everywhere in between. But with this convenience comes a key security challenge: companies must ensure that their geographically dispersed endpoints are being managed responsibly.

VMware Workspace ONE supports this effort by offering companies an intelligence-driven digital platform for securely managing employee devices, including their apps and content. Likewise, workers can carry out their duties safely and productively by using the platform's single sign-on capabilities to readily access apps from any approved device.

Used in conjunction with VMware's unified endpoint management solution and its virtual application delivery capabilities, Workspace ONE is available via subscription as an on-premise or cloud-based solution. Customers benefit by increasing end user productivity, reducing help desk costs and lowering risk.

Last year, VMware enhanced its platform with Workspace ONE Intelligence, an AI and machine learning engine that analyzes device, app and employee data in order to predictively patch vulnerabilities. The company also debuted its ONE Trust Network, a partnership of third-party solution providers whose products integrate into WorkspaceONE, thus providing additional functionality like threat detection, cloud security, analytics and authentication.

The University of Arkansas implemented Workspace ONE to help on- and off-campus students access important educational applications. Meanwhile, health care IT company Cerner improved workflow by using Workspace ONE to create a location-aware, secure SSO solution that lets medical professional quickly "tap in" with their badge when logging in to different supported devices.

Workspace ONE™

Finalists 2019

- HotShot, HotShot
- SonicWall, SonicWall Secure Mobile Access (SMA)
- ThreatMetrix, ThreatMetrix Mobile SDK
- VMware, VMware Workspace ONE
- Wandera, Secure Mobile Gateway

Trust Award

BEST NAC SOLUTION

WINNER

ForeScout Technologies, Inc. for ForeScout CounterACT

What makes ForeScout CounterACT exceptional? The fact that it doesn't make exceptions – not when it comes to monitoring and managing devices that attempt to access your organization's network.

ForeScout CounterACT provides visibility into the network activity of essentially all devices – whether they're corporate- or employee-owned, whether they contain software agents or are rogue agentless devices.

The NAC solution can see and control devices from the instant they connect, be they PCs, tablets, smartphones, industrial control systems, virtualized servers, cloud instances or IoT products. Highly scalable, the solution supports up to 2 million devices in a single deployment of ForeScout's CounterACT Enterprise Manager platform. That goes for anywhere in the extended enterprise, from traditional office spaces to data centers, the cloud and OT networks.

Because ForeScout's platform continuously monitors device connection, behavior and compliance status, users can set policies based on real-time intel, instead of relying on scheduled scans to collect point-in-time information. Better yet, the solution's heterogeneous nature means customers can generally stick with their existing network infrastructure.

In April 2018, ForeScout released a major feature update offering enhanced insights into the fastest-growing devices on enterprise networks, including IPv6 addressable systems and devices managed by cloud network controllers. Other new capabilities include passive-only monitoring for inventorying OT devices, cloud-based intelligence for auto-classifying new devices, IoT risk assessments, and a customizable device intelligence dashboard.

An IDC study found CounterACT delivers a 392 percent five-year ROI by reducing manual tasks, increasing efficiency and lowering IT costs.



Finalists 2019

- Aruba, Aruba ClearPass
- Cisco Systems, Cisco Identity Services Engine
- ForeScout Technologies, ForeScout CounterACT
- Fortinet, FortiNAC
- OPSWAT, MetaAccess

Trust Award

BEST RISK/POLICY MANAGEMENT SOLUTION

WINNER

Skybox Security for Skybox Security Suite

Companies are always looking for new and better vantage points from which they can view and manage network risk. And in that sense, Skybox Security offers the best seat in the house.

Taking home the SC Award for Best Risk/Policy Management Solution for the second consecutive year, the Skybox Security Suite platform provides organizations with the automated tools to visualize, control and reduce attack surfaces.

Key decision-makers can then implement consistent risk-reduction policies across the whole of the enterprise – on premises, in the cloud and across OT networks, as well as the end-to-end paths between networks.

The solution integrates with more than 130 networking and security technologies, normalizing and incorporating threat intelligence and vulnerability data into centralized repositories and a comprehensive network model that serves as a foundation for risk analysis, measurement, reporting and remediation.

Companies can score and prioritize risk according to their networks' specific needs, and even compare current levels with those from a previous date to see how risks have trended over time.

And they can perform same-day audits to determine if they are abiding by not only their own internal policies, but also regulatory compliance standards.

By replacing manual data collection, analysis and reporting activities with on-demand, automated processes, the security solution reduces associated costs by 90 percent, Skybox asserts.

Users with a 150-firewall deployment can also conserve an estimated $500,000 because they're able to replace manual firewall audits.



Finalists 2019

- Absolute, The Absolute Platform
- AlgoSec, AlgoSec Security Management Solution
- BitSight Technologies, BitSight Security Ratings Platform
- RiskLens, RiskLens
- Skybox Security, Skybox Security Suite

Trust Award

BEST SCADA SECURITY SOLUTION

WINNER

Dragos for Dragos Platform

The Stuxnet attack that disrupted Iran's nuclear program and the BlackEnergy malware infection that sabotaged the Ukrainian electric grid exemplified the destruction and disruption that threat actors can cause by targeting industrial control systems.

The Dragos Platform seeks to restore some piece of mind by providing ICS/OT environments with continuous monitoring of their assets and activities, while keeping them abreast of the latest adversarial threats.

Dragos essentially operates as a SIEM solution and can be deployed in a security operations center model. Its threat behavior analysis capabilities can identify and assess threats with rich contextual data, without requiring the user organization to first build a baseline profile to measure against.

The Dragos platform then combines these analytics with data imported from multiple sources, such as controller logs and data historian outputs, while also allowing alerts, IoCs and investigations to be sent to case management systems, SIEMs, and other tools through its robust APIs.

Each threat-behavior analytic is paired with an investigation playbook – created by Dragos' threat operations center – which gives step-by-step response guides for each alert in order to facilitate the investigation and mitigation process.

These playbooks can also aid the proactive hunting of hidden threats even before they are detected and an alert can be generated.

Indeed, the Dragos Platform frees security analysts to focus on the more strategic and sophisticated task of discovering new threats, leading to further efficiencies and optimization of their industrial cybersecurity posture.



Finalists 2019

- Attivo Networks, ThreatDefend™ Deception and Response Platform
- Claroty, Claroty Platform
- Darktrace Industrial, Industrial Immune System
- Dragos, Dragos Platform
- Nozomi Networks, SCADAguardian

Trust Award

BEST SIEM SOLUTION

WINNER

LogRhythm for LogRhythm's NextGen SIEM Platform

No hyperbole here: LogRhythm's NextGen SIEM Platform genuinely lives up to its name as a next-generation security tool.

The solution allows user organizations to promptly detect and respond to cyber threats before they cause damage, while identifying high-risk network activity. It unifies SIEM capabilities by bringing together network and endpoint monitoring, security analytics (UEBA, network traffic and behavior analytics, and endpoint threat detection), and security automation and orchestration.

Deployable on premises and in cloud-based and hybrid environments, the solution can collect, process, analyze and index data at a speed of more than 300,000 messages per second.

Its Machine Data Intelligence (MDI) fabric supports more than 850 systems, devices and applications and contributes critical contextual data for logging, auditing and, ultimately, analysis. LogRhythm offers scenario-based and behavior-based analytics, covering the full spectrum of known and unknown threat types.

LogRhythm's combination of automation and analytics reduces false positives, ensures consistent execution and reduces detection and response times. Meanwhile, its reporting and dashboarding capabilities allow companies to recognize workflow efficiencies and improve their overall performance.

A markedly flexible solution, the NextGen SIEM Platform offers horizontal scalability at the collection, data processing, data indexing, and analytics layers to allow customers to continue to add capacity without continually adding to overhead costs.



Finalists 2019

- Exabeam, Exabeam Security Management Platform
- LogRhythm, LogRhythm's NextGen SIEM Platform
- Rapid7, InsightIDR
- RSA Security, RSA NetWitness® Platform
- Securonix, SNYPR Security Analytics version 6.2

Trust Award

BEST THREAT DETECTION TECHNOLOGY

WINNER

Aruba, a Hewlett Packard Enterprise company, for Aruba IntroSpect

Seeking out the unusual is business as usual For Aruba, a Hewlett Packard Enterprise company.

The company's IntroSpect user and entity behavior analytics (UEBA) solution leverages AI fueled by over 100 machine learning models to detect anomalous network events and determine if the cause is an attack, exploit or breach.

IntroSpect zeros in on user, peer group and device activity that strays from established normal baselines – even if the actions are subtle or gradual. It then generates individual "risk profiles" with complete granular context to help speed investigation, prioritization and response.

Indeed, some organizations have reduced the time spent resolving single incidents from 30 hours to 10 minutes after switching from traditional threat detection methods to IntroSpect. Aruba also says customers save around $45,000 per month for 10 high-impact security incidents.

One Texas-based school district stopped an Emotet banking trojan attack in three hours with IntroSpect, while a neighboring school district without the solution suffered 10 days of downtime during the same attack period. With the malware isolated and lateral movement prevented, the district that used IntroSpect was able to preserve its business operations and its data, while pinpointing a root cause for remediation.

Recent enhancements to the solution include improved integration and analysis of third-party alerts, intelligent alert clustering, expanded visibility and analytics for privileged accounts, a streamlined analytics GUI, and more.

This is the second consecutive year that Aruba has won the SC Award for Best Threat Detection Technology.



Finalists 2019

- AlienVault, USM Anywhere
- Armis, Armis
- Aruba, a Hewlett Packard Enterprise company, Aruba IntroSpect
- CrowdStrike, Falcon Insight
- Exabeam, Exabeam Advanced Analytics
- Sophos, Sophos Synchronized Security
- Symantec, Targeted Attack Analytics (TAA)

Trust Award

BEST THREAT INTELLIGENCE TECHNOLOGY

WINNER

CrowdStrike for Falcon X

CrowdStrike has apparently vaulted us all into the future.

A January 2018 Gartner Magic Quadrant report predicted that by 2021, endpoint protection platforms "will provide automated, orchestrated incident investigation and breach response." But CrowdStrike asserts that it has already achieved this objective via its fully integrated threat intelligence and endpoint protection platform, Falcon X.

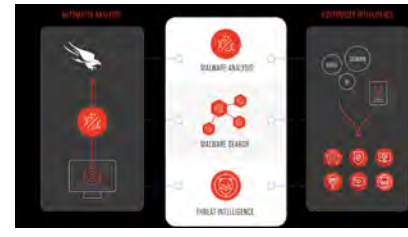
Customers of Falcon X know that its unique cloud-native architecture provides robust breach prevention capabilities with deep visibility into cyber threat intelligence, endpoint events and motivations behind adversarial behavior.

This elevates the capabilities of all security analysts and unlocks critical security functionalities for those organizations lacking a SOC operation. Benefits include more efficient incident response, improved attack prevention, increased productivity, reduced capital outlays and operating expenses, regulatory compliance, and an almost immediate time-to-value due to minimal maintenance through CrowdStrike's single-agent approach.

Falcon X enables customized and in-depth analysis of malwares and zero-day attacks, employing a unique combination of static, dynamic and fine-grained memory analysis to quickly identify threats.

The solution's malware search engine capabilities expand analysis to include all related files and variants, leading to a deeper understanding of attacks, plus an expanded set of IOCs to defend against future incursions.

In the past year, CrowdStrike has introduced data center coverage, added support for Docker containers, enabled the safe utilization of USB devices, launched a turnkey solution that combines endpoint protection technology with a dedicated team of professionals, presented additional features enabling real-time response and real-time search, and more.



Finalists 2019

- AlienVault, Open Threat Exchange (OTX)
- Comodo Cybersecurity, Comodo Valkyrie
- CrowdStrike, Falcon X
- DomainTools, Iris Investigation Platform
- Flashpoint, Flashpoint Intelligence Platform
- Recorded Future, Recorded Future
- RiskIQ, RiskIQ PassiveTotal

Trust Award

BEST UTM SECURITY SOLUTION

WINNER

Fortinet for Fortinet Unified Threat Management Solution

When you build your network security defenses in piecemeal fashion, you risk ending up with some pieces that don't quite fit.

For those wishing to avoid that fate, the Fortinet Unified Threat Management Solution offers an affordable and manageable all-in-one UTM solution that truly stands out for its tight and seamless integration.

It does the job of at least eight individual security products that would normally require their own separate management – including traditional firewalls, intrusion prevention systems, gateway antivirus, web filtering, secure email gateways, sandboxes, web application firewalls and CASB solutions.

Originally, UTM solutions traditionally combined network security, email security and web security together into a single solution. But more recently, the definition of UTM has expanded to include wired and wireless networking, integrated endpoints, sandboxing, additional networking extensions and cloud-based management.

Fortinet has all that covered, offering extensive routing, switching, access control, Wi-Fi, LAN and WAN capabilities – all with tight cross-network and endpoint integration.

Fortinet's FortiGate UTM appliances offer high-performance SSL inspection capabilities for web- and cloud-based services. And as one of the first UTM vendors to offer SD-WAN functionality, Fortinet reduces WAN complexity and operating expenses, allowing companies to monitor and route traffic based on quality of service while improving and securing the performance of SaaS applications.

To date, Fortinet has shipped more than four million UTM appliances to more than 350,000 customers.



Finalists 2019

- Fortinet, Fortinet Unified Threat Management Solution
- Secucloud, Secuscaler
- SonicWall, SonicWall NSa Series
- Sophos, Sophos XG Firewall
- WatchGuard Technologies, WatchGuard Firebox M270

Trust Award

BEST VULNERABILITY MANAGEMENT SOLUTION

WINNER

Tenable for Tenable.io

The larger and more unwieldy an organization's digital attack surface becomes, the more likely its internal cyber risk assessments will suffer from key oversights and omissions.

Recognizing this "Cyber Exposure Gap," Tenable created Tenable.io, a cloud-based vulnerability management solution that uses passive network monitoring, active scanning and an endpoint agent to comprehensively evaluate assets within a business infrastructure. Capable of tracking over 1 million assets per customer, Tenable.io covers a full spectrum of devices, including servers, laptops, web applications, IoT products and operational technology.

Even dynamic and short-lived IT assets such as cloud instances and containers are fully supported – while Tenable's elastic asset licensing models reduce cost because companies aren't required to pay for ephemeral assets that no longer exist. The ability to remediate container security risks is especially noteworthy because of how the product integrates directly into the DevOps pipeline, allowing problems to be discovered before they ever reach production.

Meanwhile, an integrated SDK and API collectively allow companies to build on Tenable's platform and automate the sharing of asset/vulnerability information within their networks.

Since the solution's debut, Tenable has added a container security application, web application scanning, and enhanced detection for ICS/SCADA systems (in partnership with Siemens).

Additionally, the company began a beta test of its Tenable.io Lumin visualization, analytics and measurement solution, which combines raw data with business asset criticality and threat context, helping CISOs better measure and communicate cyber risk.

Tenable is backed by its research team, which recently discovered more than 40 zero-day vulnerabilities over a two-year period.



Finalists 2019

- Checkmarx, Software Exposure Platform
- Denim Group, ThreadFix
- Digital Defense, Frontline VM™, a Frontline.Cloud™ system
- Rapid7, InsightVM
- Tenable, Tenable.io

Trust Awards

BEST WEB APPLICATION SOLUTION

WINNER

Akamai Technologies for Kona Site Defender

Now here's an app protector deserving of your app-lause and appreciation.

Akamai Technologies' Kona Site Defender is a cloud-based solution that insulates websites, mobile apps and their APIs against a wide range of threats, blocking them at the edge before they can breach key servers and systems.

Earning points for its customization, scalability and accuracy, Kona Site Defender helps safeguard some of the Internet's most popular websites and Internet-facing applications from defacements, data theft, DDoS attacks and other malicious activity.

Central to Kona Site Defender is its web application firewall that reduces risk of attacks and exploits in real time, while tailoring its protections and applying new rules based on a particular website's ongoing traffic patterns. Customers can manage their protections from a single location and do not have to place staff in every data center, even as the number of applications grows.

The solution draws resources from Akamai Technologies' worldwide infrastructure, including 235,000 servers and 2,400 data centers, as well as its globally distributed 24/365 Security Operations Center, which helps with security monitoring and attack support and mitigation.

Akamai has visibility into 15-to-30 percent of the world's web traffic, and Kona Site Defender uses that data to gather threat intelligence and test its WAF rules.

Customers can further enhance their defenses with optional add-ons, including a client reputation module that generates a risk score for every source IP address, a "Bot Manager" tool, and Akamai's Fast DNS service that offloads DNS resolution from one's infrastructure to the cloud.



Finalists 2019

- Akamai Technologies, Kona Site Defender
- Contrast Security, Contrast Protect and Assess
- Imperva, Imperva Web Application Firewall (WAF)
- ThreatX, Threat X WAF
- WhiteHat Security, WhiteHat Application Security Platform

Excellence Award

BEST CUSTOMER SERVICE

WINNER

Endgame

Endgame doesn't waste any time getting to the bottom of its clients' technical support needs, offering a seemingly endless array of speedy and helpful customer service offerings to organizations that deploy its endpoint security platform.

Its technical support team is composed entirely of Tier 3+ support engineers – nothing lower. Rather than escalating the customer through a series of contacts, Endgame instead makes sure that the person who answers the call is qualified to resolve the issue.

Customers can seek support via telephone, email or online portal. On-site help is also available at additional cost.

"It gives me peace of mind to know that I have the best security analysts in the world just a phone call away at Endgame – and that the analyst that responds to our support ticket is the one that will fix the problem, period," says Endgame user Matthew Witten, information security officer at Martin's Point Health Care in Portland, Maine.

With testimonials like that, it's no wonder Endgame boasts a 100 percent customer satisfaction score.

Of course, Endgame aims to reduce the number of tech support tickets in the first place by providing customers with troves of easily digestible documentation to support product installation and operation. Authored by skill tech writers, this helpful content is built directly into the product user interface for ease of access.

The company's Customer Success portal similarly hosts documents, FAQs, user guides and pro tips to aid with topics such as installation, system requirements, compatibility and troubleshooting.

Endgame provides its clients with product trial support, remote implementation support, and a learning management system that features live coaching. Customers can also join Endgame product user groups to ask key questions or hear about product updates.



Finalists 2019

- Barracuda Networks, Barracuda Customer Service
- Cofense, Cofense Support/Technical Operations Center
- Endgame, Endgame
- Entrust Datacard, Entrust Datacard Customer Service Team
- Zix, Zix Solutions

Excellence Award

BEST EMERGING TECHNOLOGY

WINNER

StackRox for StackRox Container Security Platform

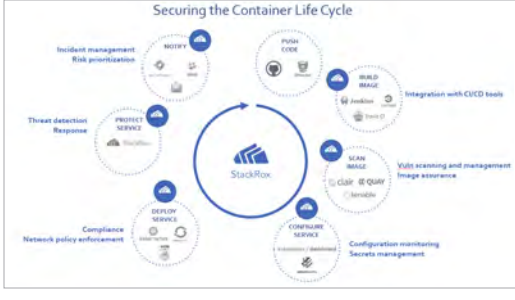
The growing popularity of container technology has created a gaping hole in the cybersecurity sector that Stackbox is more than happy to fill.

Containers and cloud-native applications possess unique architectural traits that pose visibility challenges for traditional security tools and perimeter defense systems. The volume of activity for containers is far higher than that of traditional monolithic applications. And communications between containers as well as container orchestrators present new attack surfaces.

Debuting in mid-2017, the StackRox Container Security Platform is designed specifically to secure containers and cloud-native development stacks in use on private and public cloud infrastructures. Deploying as a set of automated container-based microservices via the open-source Kubernetes orchestration platform, the solution enables users to visualize the container environment, generate risk profiles, reduce the attack surface, and adaptively detect and stop malicious activity.

StackRox's customer base includes major banks, fintech companies, e-commerce app providers and security services companies. StackRox also entered into an agreement with In-Q-Tel, a not-for-profit strategic investor that accelerates the development of cutting-edge technologies employed by U.S. government agencies and the intel community.

Peer-to-peer fintech company Lending Club deployed StackRox because it needed to move to containers to develop its financial services applications faster. "The visibility StackRox provided gave us valuable insights right away," says Brian Johnson, Lending Club's former CISO. "StackRox shows us where we've misconfigured containers to have higher privilege levels than needed, so we can reduce our attack surface."



Finalists 2019

- Cipher-Cloud, CipherCloud CASB+
- empow, empow Cyber Security
- Mimecast, Mimecast Awareness Training
- StackRox, The StackRox Container Security Platform
- Whistic, Whistic Security Profile

Excellence Award

BEST ENTERPRISE SECURITY SOLUTION

WINNER

CyberArk for CyberArk Privileged Access Security Solution

Privileges have their benefits… and their burdens.

The more access users have to their companies' critical systems, the more damage attackers can cause if they compromise their credentials or accounts.

That's why the CyberArk Privileged Access Security Solution is specifically designed to detect and prevent attacks on privileged user accounts and sessions across an organization's entire network, including on-premises, cloud-based, DevOps, IoT and even RPA (robotic process automation) environments.

With more than 4,000 customers, CyberArk is constantly focused on efficiently delivering the highest levels of security, recoverability and auditability at a low total cost of ownership.

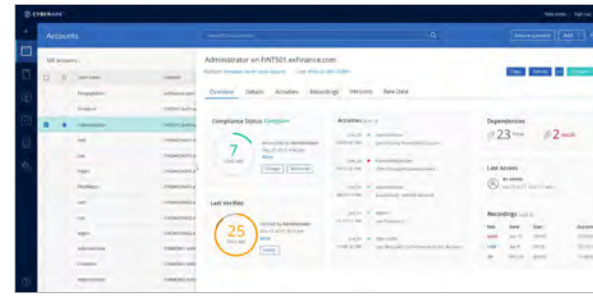
The latest version of its PAM solution, v10, delivers a 10x improvement in time spent on privileged account-related tasks, and a 5x reduction in the time auditors spend reviewing session records.

In its ongoing commitment to keep pace with recent evolutions in networking, CyberArk in 2018 acquired technology from Vaultive to deliver greater visibility and control over privileged admins and users in cloud-based environments.

Last year, CyberArk announced the availability of its CyberArk Privilege Cloud, a new privileged access security-as-a-service offering.

The company also recently expanded its MSSP offerings, and even launched its own CyberArk Marketplace, which offers a broad portfolio of privileged access integrations.

Those are just some of the latest breakthroughs for a pioneering company whose past accomplishments include becoming the first privileged account security vendor to achieve Common Criteria Evaluation Assurance Level EAL 2+.



Finalists 2019

- Cisco, Umbrella Secure Internet Gateway
- CyberArk, CyberArk Privileged Access Security Solution
- Proofpoint, Proofpoint Advanced Email Security
- Recorded Future, Recorded Future
- Vectra, Cognito Platform

Excellence Award

BEST REGULATORY COMPLIANCE SOLUTION

WINNER

OneTrust Privacy Management and Marketing Compliance Platform

The privacy management software market may still be in its infancy, but already the OneTrust Privacy Management and Marketing Compliance Platform has become a leader in this emerging category as it helps user organizations survive a rising tide of global regulations.

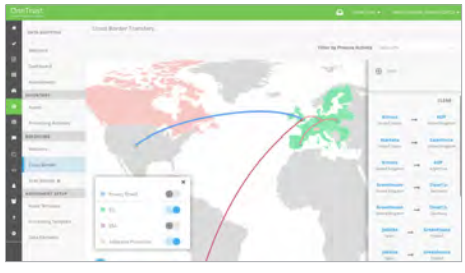
More than 1,500 customers use OneTrust to comply with regulations such as GDPR, ePrivacy and the California Consumer Privacy Act – with an additional 10,000 organizations using the technology through a partnership with the International Association of Privacy Professionals.

OneTrust's platform allows customers to modularly build out their privacy compliance toolset according to their current needs and future growth strategies. It enables data protection by design and default, data protection impact assessments, vendor risk management, incident and breach management, targeted data discovery, data mapping, consent management, ePrivacy cookie consent, data subject access rights, portability and the right to be forgotten.

To meet its market needs, OneTrust scaled to over 500 employees in under three years. Additionally, the company is expanding its international presence with new local data centers and six global offices.

Customers can deploy on premises or in an EU-cloud and can easily upgrade and scale platform capabilities as their privacy programs mature.

"OneTrust modules gives us the flexibility and customization to tackle GDPR one step at a time," says Rekha Kothamachu, director of data integration and reporting at the international travel agency network Virtuoso. "We started with cookies and are moving on to DPIAs, data subject requests and more."



Finalists 2019

- Netwrix Corporation, Netwrix Auditor
- OneTrust, OneTrust Privacy Management Software
- RSA Security, RSA Archer Regulatory & Corporate Compliance Management
- Tripwire, Tripwire Enterprise
- Varonis, Varonis Data Security Platform

Excellence Award

BEST SECURITY COMPANY

WINNER

Fortinet

Fortinet recently reached a huge milestone, surpassing over 500 cybersecurity technology patents worldwide, with hundreds more pending.

It's this commitment to innovation that allows the company to cover growing attack surfaces like a blanket, across conventional networks as well as IoT, OT, and cloud environments.

To stay cutting edge and keep pace with its growth, Fortinet is expanding its headquarters and R&D Center in Sunnyvale, Calif. This facility represents the home base of the FortiGuard Labs team, which leverages leading-edge machine learning and AI technologies to develop threat intel that feeds the company's solutions, used by more than 360,000 global customers.

Collectively, Fortinet's solutions and services comprise its Security Fabric, an open-architecture tech approach that improves network visibility and automates threat response by uniting and integrating key security technologies across endpoints, network access points and email and web applications.

These solutions are then enhanced through the integration of advanced threat protection technologies and a unified correlation, management, orchestration and analysis system.

Meanwhile, the Fortinet Network Security Academy program provides industry-recognized cybersecurity training and certification opportunities to students around the world. Launched in 2016, this rapidly growing program has already been adopted by 105 academies in 49 countries.

Fortinet also spreads cyber awareness through its Network Security Expert (NSE) Program, an eight-level training and assessment program designed for customers, partners and employees, with over 138,000 security certifications at the time of the company's nomination.



Finalists 2019

- Carbon Black
- Checkmarx
- Contrast Security
- CrowdStrike
- Darktrace
- Fortinet
- Illumio

Elevate your Vulnerability Management Results with Frontline.Cloud

Each day, more and more security technologies are touting their “cloud” features. At Digital Defense, Inc. we take pride in the fact that we have been delivering services through our cloud-based technology long before it was a common practice. Call us visionaries, but we saw the benefits that a cloud solution brought to our clients, and made the commitment to developing the most accurate, nimble and innovative security assessment technology from Day 1.

FRONTLINE VM™

FRONTLINE ATS™

FRONTLINE WAS™

FRONTLINE Pen Test™

FRONTLINE.CLOUD

Born in the Cloud. Built for the Cloud.

TRUST THE ORIGINAL CLOUD SECURITY PROVIDER

Innovative Technology and Expertise

- Patented Scanning Technologies
- Highly Accurate, Low Abrasion Scans
- Patented Scan to Scan Host Tracking
- Frontline Security GPA® Grading System

Industry Recognized

TSR The SaaS Report TOP 25 CYBERSecurity Companies 2018

CRN MSP 500 2018

TAG cyber 2019 DISTINGUISHED VENDOR

Diverse and Easy to Implement Solutions

- Automated Threat Hunting
- Vulnerability Scanning
- Web Application Scanning
- Penetration Testing

888-273-1412

DIGITAL DEFENSE INCORPORATED

DigitalDefense.com

Excellence Award

BEST SME SECURITY SOLUTION

WINNER

AlienVault for USM Anywhere

AlienVault's "USM Anywhere" Unified Security Management platform has taken giant strides protecting not-so-giant businesses.

The cloud-based SaaS threat detection solution is ideal for small- and medium-sized businesses with limited resources and manpower. It delivers myriad enterprise-wide security capabilities into a single, centralized solution, increasing productivity by 80 percent.

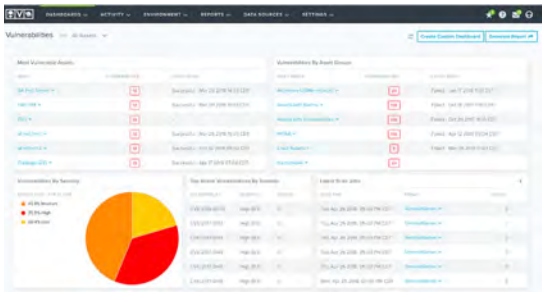
Jason Harper, founder and CEO of the web-based payment application Celopay, said deploying USM Anywhere "allowed us to consolidate what would be, traditionally, multiple security roles... parsing information and monitoring it on a day-to-day basis."

Meanwhile, the solution also eliminates the need to invest in dozens of point products that add to the bottom line, not to mention data centers, hardware, setup fees and maintenance costs.

USM Anywhere leverages a continuous stream of threat intel gleaned from AlienVault Labs as well as the Open Threat Exchange's community of over 70,000 threat researchers and security professionals. According to a commissioned Forrester study, deploying USM Anywhere delivered a 6x return on investment to customers over three years and a savings of more than $40,000 annually in threat intelligence expenses.

The platform allows users to introduce additional security controls, without any complex integrations or product upgrades, via AlienApps, which are modular integrated software components that extend USM Anywhere's capabilities to third-party applications.

Customers with tech support or configuration issues can communicate directly with an AlienVault Certified Expert to quickly resolve their challenges. And during implementation, they can take advantage of "LiftOff Packages" that include services and training to help them get up and running.



Finalists 2019

- AlienVault, USM Anywhere
- Barkly, Barkly Endpoint Protection Platform
- Malwarebytes, Malwarebytes Endpoint Protection
- SiteLock, SiteLock® SecureSite
- Webroot, Webroot SecureAnywhere

Excellence Award

ROOKIE SECURITY COMPANY OF THE YEAR

WINNER

Axonius

It's only been a year since Israeli start-up company Axonius introduced its cybersecurity asset management platform to the world, and the accolades are already piling up.

Axonius gives user organizations the ability to uniquely identify users and their devices, and then take appropriate action if they are not following proper security policies. Contextual device information includes device type, known vulnerabilities, logged-in users, available patches and full histories.

Just about every company has a rogue device somewhere. Axonius has discovered that 10 to 18 percent of its customer base's user devices are unmanaged, while 16 to 24 percent of its clientele's devices are missing an endpoint solution that's already been paid for. And 100 percent of Axonius' customers have found users with incorrect permissions or devices on their networks that they weren't even aware of.

One global enterprise client with 150,000 employees was particularly stunned by the platform's ability to show users with admin rights that hadn't changed their passwords in years.

Customers benefit by efficiently driving their mean inventorying time from 10 minutes or more per incident to mere seconds. Installation is also streamlined, as the product can be up and running in minutes.

"Axonius has found a truly innovative way to crack the code around solving the security practitioner's most glaring problem: how to identify the assets they are charged with protecting," says customer Jim Rutt, CIO at Dana Foundation, a philanthropic organization that supports brain research. "Their unique approach of integrating key applications ensures a 360-degree view of the organization's technology assets and, more importantly, the relationships between these assets to form a holistic foundation by which an organization can base its security strategy."



Finalists 2019

- Axonius
- Cyberstone
- Intezer
- Minerva Labs
- PasswordPing

Professional Award

BEST CYBERSECURITY HIGHER EDUCATION PROGRAM

WINNER

University of Maryland University College

The key to operating the finest cybersecurity teams in the world is diversity. Team members need to be from diverse backgrounds, and their areas of expertise must encompass a wide spectrum of specialties and interests.

This philosophy, which the University of Maryland University College (UMUC) has fully embraced, is among the driving reasons the school was chosen for the second consecutive year as the winner of SC Media's Best Cybersecurity Higher Education Program.

UMUC's Master of Science in Cybersecurity Technology graduate program welcomes students who previously majored in criminal justice, human resources, psychology, politics, criminal justice, law, and even linguistics and art – with no GRE or other barriers to entry. The program then melds these students into teams to approach the subject matter through an interdisciplinary lens.

Because understanding how to work as a group is one of the program's cornerstones, the students ultimately learn from each other as much as they do from the curriculum and professors.

Another of UMUC's key approaches is to train students how to think and function in a professional business environment. Lessons range from the basics of preparing executive presentations to recording podcasts – which is immensely helpful, as UMUC has partnered with several large federal government and private business organizations to provide job opportunities to students and graduates.

The UMUC program is certified by NSA and DHS as a Center of Academic Excellence in IA Education, and won (ISC)²'s Americas 2017 Information Security Leadership Award. Some of the school's faculty members work for such prestigious employers as the NSA, Lockheed Martin and Leidos, while others have served on presidential advisory councils or in CIO roles with public and private organizations.



Finalists 2019

- Champlain College
- New York University
- University of Maryland University College (UMUC)

Professional Award

CYBERSECURITY STUDENT OF THE YEAR

WINNER

Kyle Joseph Baldes, Oregon State University

In a matter of six months, Oregon State computer science student Kyle Baldes transformed himself from security neophyte to an artificial intelligence expert presenting proprietary research findings to senior cyber executives.

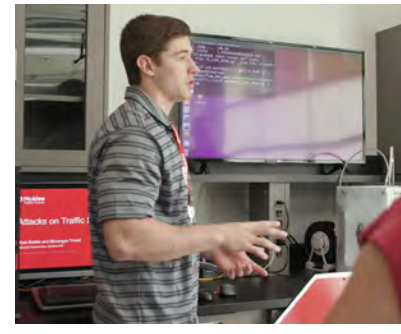
During an extended internship with McAfee's Advanced Threat Research (ATR) team, Baldes leveraged adversarial machine learning techniques to investigate flaws in deep learning models used by self-driving vehicles. He developed both a digital and physical exploit to trick autonomous vehicle sensor systems into misidentifying a stop sign as other traffic signage, such as a speed limit sign.

The digital version works by adding a small amount of noise, or perturbation, to images of stop signs in order to trick the signage classifier. For the physical attacks, Baldes placed specially-crafted stickers on stop signs that would cause the signs to be incorrectly classified.

"The results demonstrated the vulnerability of deep neural networks and provided insights for defense and protection," says Catherine Huang, a senior data scientist responsible for advanced analytics research at McAfee.

As he completes his degree, Baldes will continue to work with the ATR team, which will use his research findings to test physical attacks on production automotive systems and then develop defenses to counter such scenarios. Additionally, he will leverage his newfound knowledge to lead research efforts at OSU to identify and resolve flaws in facial recognition systems and malware detection mechanisms.

"Kyle is without question the hardest working and most capable intern I have had the pleasure to work with," says Steve Povolny, head of ATR at McAfee. From day one his commitment, resolve and ability to learn at a staggering pace impressed me greatly."



Finalists 2019

- Kyle Joseph Baldes, Oregon State University
- Nick Gregory, New York University
- Philip Smith, Texas A&M University System
- Casey Stephens, Texas A&M Engineering Experiment Station

Professional Award

BEST IT SECURITY-RELATED TRAINING PROGRAM

WINNER

Circadence for Project Ares

Meet Athena, the natural language-processing AI system that serves as a host and advisor to trainees learning on Circadence Corporation's Project Ares cybersecurity training and assessment platform.

Athena provides guidance and assessments to academic, corporate and government professionals who use Project Ares to learn how to defend their networks against critical threats to their systems. The use of AI eliminates the need for human classroom instructors, allowing trainees to learn on their own time, 24/7, either on premises or in cloud-based environments.

Project Ares "gamifies" its lessons to keep professionals engaged and motivated, while also improving knowledge retention. Trainees are tasked with offensive and defensive missions in realistic virtual environments featuring real-world tools on emulated company networks. The platform bases its simulated threat scenarios on recent real-life attacks, and keeps training relevant to users by basing it on their individualized learning behaviors.

Trainees can participate in red and blue team missions to earn badges, with results posted on a leaderboard. Or they can partake in challenges, inspired by card and strategy games, that employ repetitive learning techniques to help reinforce good habits.

Lesson objectives are based on frameworks established by both NIST and the National Institute for Cybersecurity Training. Once employees complete their regimens, managers can review their performance to evaluate skills gaps and risk.

"Project Ares is innovative in its simulation of the attacker and provides means to allow the defenders to think out of the box," says Tunde Oni-Daniel, head of information security at Perdue Farms, Inc., a Circadence customer. "It also ensures that the how-tos are included to provide the attacker and defender quick info to solve exercises."



Finalists 2019

- Circadence, Project Ares
- KnowBe4
- Las Vegas Valley Water District
- Secure Code Warrior
- Wombat Security, a division of Proofpoint

Professional Awards

BEST PROFESSIONAL CERTIFICATION PROGRAM

WINNER

(ISC)² for CISSP certification

SC Media isn't the only one celebrating a 30th anniversary in 2019.

For three decades now, the Information System Security Certification Consortium – or (ISC)²– has been offering cybersecurity professionals worldwide access to unparalleled education, as well as career enhancement opportunities such as networking and mentoring.

Nearly 120,000 cyber professionals are now CISSP-certified, meaning they are proficient in eight core cyber concepts.

At the time of its release, (ISC)²'s 2017 Global Information Security Workforce Study found that CISSP-certified members earned an average annual salary of $109,000 – 36 percent more than non-members. Indeed, a CISSP certification is considered a huge leg up for prospective employees, if not an outright requirement. Case in point: a recent search of "CISSP" on Monster.com turned up 9,000 job postings.

Every three years, members must register for an additional 120 continuing education credits. To that end, (ISC)² offers both in-person and virtual education for its members, with 126 regional chapters serving 18,000 cybersecurity professionals worldwide.

CISSPs tend to share their knowledge – about 1,000 have volunteered to educate more than 200,000 students.

James McQuiggan, product and solution security officer, Americas, at Siemens Gamesa, says that (ISC)² provides a "wealth of opportunities" to "stay current on best practices, standards and regulations, and also to network with the best professionals in the information security community."

A certification "helps me to be taken more seriously when dealing with the IT organization," says Natalia Hanson, technical audit senior director at Nasdaq. "Especially since I am a woman" and IT organizations are "often male-dominated."



Finalists 2019

- (ISC)², CISSP
- ISACA
- ISACA
- Cloud Security Alliance
- OneTrust



THREAT INTELLIGENCE EXCLUSIVELY FOR EVERYONE

Recorded Future

www.recordedfuture.com

Professional Award

BEST SECURITY TEAM

WINNER

Kimberly-Clark for its Cyber Security & Assurance team

It turns out Kimberly-Clark is as adept at cyber hygiene as it is at personal hygiene.

The $18 billion consumer product goods company founded its Cyber Security & Assurance (CS&A) global information security program in 2015 after hiring its very first CISO. Since then, the team has been following NIST guidelines as it builds out its security ecosystem while developing a culture of cyber awareness.

A lot is at stake. KC must protect more than 1,200 branded websites and mobile apps, over 90 mill locations, 56,000 employees and hundreds of thousands of devices.

Recent projects include a unified cloud computing initiative, an information classification and handling program, and a hosted information risk assessment (HIRA) for third-party vendors. That's in addition to day-to-day responsibilities such as protecting senior management from phishing and social media attacks, and remaining in compliance with data privacy regulatory requirements.

"Our General Data Protection Regulation team could always rely on CS&A to ensure our software systems are protecting our consumer and staff data according to the highest standards of the law," says Fionn Herriot, Kimberly-Clark's Ethics & Compliance manager for the EMEA Region, adding that CS&A "continues to be instrumental in communicating the changes, training, upgraded capabilities and tools available to hundreds of GDPR stakeholders across the company."

To ensure its workforce remains vigilant, KC this year debuted its mandatory cybersecurity awareness training and assessment program, which uses gamification techniques to teach employees to recognize and avoid social engineering scams. Additionally, the company's threat intelligence team distributes weekly updates to keep workers abreast of the latest threat activity.



Finalists 2019

- Kimberly-Clark
- Lincoln Financial
- Penn Medicine
- Welltok

Professional Awards

CSO OF THE YEAR

WINNER

Peter Liebert, CISO and Director of the Office of Information Security, California

Two years ago, California didn't have a centralized IT security team. Each of the Golden State's 138 government departments, agencies and branches separately managed its own security operations. Unfortunately, some of these entities turned into "islands of neglect," according to Peter Liebert, who was named California's CISO in November 2016. To ensure consistent security practices across the state government's wide-area network, Liebert fast-tracked the building of a fully functional 24/7/365 Security Operations Center in just seven months. In the calendar year after its deployment, California's brand-new suite of security systems confirmed over 100 incidents that once would have gone undetected.

Liebert built up the Office of Information Security (OIS) team from a core of nine staff members to nearly 60 security pros, with zero job turnover, and boosted the budget tenfold.

His organization has overseen nearly 100 technical independent security assessments identifying thousands of vulnerabilities. OIS also played an integral part in migrating the entire state's email system to Microsoft Office 365 and incorporating advanced threat prevention features into it, having, the California Highway Patrol says, "the most pronounced net positive impact to reducing the phishing threat the state has ever seen."

OIS instituted a centralized anti-phishing training service, debuted California's first Information Security Leadership Academy and formed an in-house dedicated cybersecurity advisory team to aid high-risk state entities Liebert's influence extends to other states as well – his California Cybersecurity Maturity Metric (CCMM), which objectively measures a cybersecurity program implementation, was posted by the National Institute of Standards and Technology (NIST) for other states to use.



Finalists 2019

- Peter Liebert, CISO, California Department of Technology
- Timothy Lee, CISO, City Of Los Angeles
- Pat Lefemine, SVP, CISO, Lincoln Financial Group
- Dan Costantino, CISO, Penn Medicine
- Pritesh Parekh, VP, CSO, Zuora

zix | appriver

Sophisticated attacks demand a sophisticated solution vendor. With effortless email security and phenomenal support, Zix keeps your email, employees, and business safe from the latest threats.

- **ADVANCED THREAT PROTECTION**

  Multi-layer filters combine with live threat analysts and sophisticated machine learning to create a system that accurately prevents malicious email threats

- **UNIFIED ARCHIVING**

  Secure email and electronic communications archiving for compliance and eDiscovery

- **EMAIL ENCRYPTION**

  Automatic, policy-based email encryption offering TLS, transparent, pull and push delivery methods

At Zix, our security and compliance experts are here for you. We can help you defend against the latest inbound email threats, secure your data in outbound email, ease archiving and eDiscovery, and maintain the lead efficiency of your IT team.



Professional Award

EDITOR'S CHOICE AWARD

WINNER

The FIDO Alliance

Authenticating your identity should be as easy as 1-2-3. Unfortunately, some users take that philosophy a little too literally, using 1-2-3-4-5 or something equally insecure as their passwords when logging in to web-based services or applications.

The FIDO ("Fast IDentity Online") Alliance has made it its mission to phase out the use of outdated password technology, and replace it with cryptographically secure, standards-backed authentication alternatives such as on-device biometrics and FIDO Security Keys. And 2018 was landmark year in the open industry association's effort to accomplish that very goal.

In conjunction with the World Wide Web Consortium (W3C), FIDO last April officially launched the FIDO2 Project, a set of interlocking initiatives that together create a FIDO Authentication standard for the web. FIDO2 encompasses both the W3C's Web Authentication specification (WebAuthn) and the FIDO Alliance's Client-to-Authenticator Protocol (CTAP).



Combined, WebAuthn and CTAP help users leverage common devices to achieve hassle-free authentication in both mobile and desktop environments. According to the Alliance, FIDO2 supports passwordless, second-factor and multi-factor user log-in experiences that leverage embedded/bound authenticators such as biometrics or PINs, or external/roaming authenticators like FIDO security keys, mobile devices and wearables.

Many of the world's most popular browsers and operating systems platforms have moved quickly to take advantage. Indeed, FIDO2 technologies are already built into the latest versions of Windows 10, Google Play Services on Android, and the Chrome, Firefox and Edge web browsers. WebKit, the technology behind Apple's Safari web browser, is also previewing support for FIDO2, and just last month, Google announced that Android is now FIDO2-certified.

The FIDO Alliance helped pave the way for adoption of its specifications by providing various testing tools for platform developers, and also by launching a FIDO2 certification program. A certification means that a product not only complies with FIDO2 specifications, but also is interoperable with other FIDO2 products.

In September 2018, the first crop of FIDO2-certified authentication products were made available from such organizations as CROSSCERT: KECA (Korea Electronic Certification Authority); Dream Security Co., Ltd. Korea; ETRI; eWBM Co., Ltd.; IBM; Infineon Technologies; INITECH Co., Ltd.; Nok Nok Labs; OneSpan; Raonsecure; Samsung SDS; Singular Key; Whykeykey Inc.; Yahoo Japan Corporation; and Yubico. This included the first universal FIDO server, which supports not only all FIDO2 authentication devices but also those running on earlier open authentication standards UAF and U2F, enabling backward compatibility for any previously certified FIDO authenticators.

Companies pursuing biometrics-based authentication were further helped by FIDO's September 2018 launch of its Biometric Component Certification Program, the first in the industry program designed to certify that biometric recognition systems successfully meet globally recognized performance standards and are viable for commercial use. The program delivers significant time and cost savings to biometrics vendors because it enables them to test and certify their technology only once in order to validate their system's performance, and then repeatedly re-use that third-party validation across their potential and existing customer base.

Even before the official launch of FIDO2, the Alliance expanded its previously established certification program to include multi-level security evaluations for authenticator technologies. In a press release at the time, FIDO Alliance Executive Director Brett McDowell said that the new and improved certification program "enables enterprises and online services to make better informed risk management decisions when registering credentials from FIDO-enabled devices, resulting in more accurate and reliable scores on the back-end while delivering better user experiences on the front end due to lower instances of intrusive 'step up authentication' challenges."

Just last December, the FIDO Alliance reached what is arguably the highest bar set in information and communication technology (ICT) standardization when the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) recognized UAF 1.1 and CTAP as international standards.

SC 2019 awards

Honored in the U.S.

Haymarket Media
275 Seventh Avenue, 10th Floor
New York, N.Y. 10001
Email: scfeedbackus@haymarketmedia.com
Telephone: 646-638-6008
Fax: 646-638-6150
Web: www.scmagazine.com

#scawards