SC 2017 awards
EUROPE

Tuesday, 6th June 2017
Old Billingsgate
1 Old Billingsgate Walk, London
EC3R 6DX

Surviving a tough year

Welcome to the SC Europe Awards Book of the Night 2017. After another tumultuous year in cyber-security, we are delighted to be celebrating our worthy winners.

What a year it's been. Our trusted 'things' were turned against us by the Mirai botnet, resulting in the biggest DDoS attacks seen to date. And NSA cyber-espionage tools have been used to create WannaCry, which brought NHS hospitals and other critical organisations worldwide to their knees.

Meanwhile, the Russians were widely blamed for hacking to influence the US election, while North Korea, China, Iran and the so-called Islamic State – continue to pose a significant threat.

But against this onslaught our tireless efforts in cyber-defence have also reaped rewards. We have witnessed advances in many areas, from the use of digital forensics tied to big data and AI to increased cooperative initiatives such as NoMoreRansom. Our thinking has moved beyond the perimeter. While we continue to strengthen our endpoints and ID access, we are also improving our ability to detect intruders, mitigate their activities, eject them swiftly and ensure our systems are robust enough to ensure operational resilience. Defenders are constantly honing their skills, and are more likely to spot and be able to remediate network incursions, reducing the opportunity to monetise cyber-crime, minimising the impact of data breaches and restoring systems more quickly and effectively.

Occasionally our diligence yields a lucky break. Marcus Hutchins, aka MalwareTech, found a kill-switch, which halted the spread of WannaCry thanks to doing a thorough job.

Whether it's incremental improvements or breakthrough moments, we are delighted to recognise and celebrate our successes in this year's awards.

Congratulations to you all.

– Tony Morbin, Editor-in-chief, SC Media UK

SC 2017 awards EUROPE

Contents

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
EDITOR-IN-CHIEF Tony Morbin
tony.morbin@haymarket.com
DEPUTY EDITOR Tom Reeve
tom.reeve@haymarket.com
REPORTER Max Metzger
max.metzger@haymarket.com
TECHNOLOGY EDITOR Peter Stephenson

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
PRODUCTION EDITOR Danielle Correa
danielle.correa@haymarketmedia.com

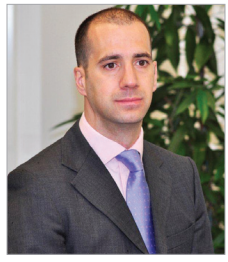
EVENTS
EVENTS COORDINATOR Sophia Edie
sophia.edie@haymarket.com
ONLINE COMMUNITY MANAGER
Roi Perez
roi.perez@haymarket.com

PUBLISHING
PUBLISHING MANAGER Gary Budd
CHIEF EXECUTIVE Kevin Costello

UK SALES
VP, GROUP PUBLISHER David Steifman
david.steifman@haymarketmedia.com
DIRECTOR, GLOBAL SALES
Dennis Koster
dennis.koster@haymarketmedia.com
UK ACCOUNT DIRECTOR Martin Hallett
martin.hallett@haymarket.com

The Judges

Rory Alsop
group head of info security oversight, Metaltech



Dean Atkinson
director of IT security, Burberry

Martyn Croft
chief information officer, The Salvation Army UK

Michael Everall
deputy chief risk officer/ head of infosecurity (international), Fidelity National Information

Stephan Freeman
CISO, Telegraph Media Group

Peter Gibbons
head of IM security, Network Rail

Steve Hindle
senior director, global security operations, Sykes

Bridget Kenyon
head of information security, UCL

Elena Kvochko
CIO, group security function, Barclays Bank

Tim Lansdale
head of payment security, WorldPay

Mike Loginov
CIO & CISO, Ascot Barclay Group Ltd

Stephen Murgatroyd
director of operations, Institute of Operational Risk

Philip Owen MBE
global head of information security, IHS Markit

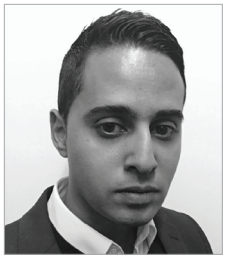
Margaret Patrick
VP and IT manager, XL Capital Ltd

Robert M Rodger
group head of security technology & architecture, HSBC Holdings Plc

Brian Shorten
chairman, Charities Security Forum

Bob Tarzey
founder, QuoCirca

Quentyn Taylor
director of EMEA information security, Canon-Europe



Mudassar Ulhaq
CIO, Waverton Investment

Marc White
CISO, Optomany

Emma Wright
partner, technology lawyer, Kemp Little

The Sponsors

SC Media UK thanks all sponsors for their generous support of the 2017 SC Awards Europe. This event, which helps raise professional standards in the information security industry worldwide, was made possible thanks to their involvement.

Boole Server is the first Italian provider of data-centric solutions, customised for small and big businesses. Thanks to military-level encryption, Boole Server provides its customers with data protection solutions. BooleBox technology, secure sync and share platform, is able to give full control of a user's data, helping to avoid non-authorised access, thanks to user-friendly protection tools. Now Boole Server products are distributed in over 25 countries, through a growing partners network. Boole Server can count on over 180 premium customers – among them Qatar Airways, Riyadh Bank, State of Jersey Police, Banco BPM – and more than 100.000 worldwide users.

Carbon Black has designed the most complete next-gen endpoint security platform, enabling organisations to stop the most attacks, see every threat, close security gaps, and evolve their defences. The Cb Endpoint Security Platform helps organisations of all sizes, replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 customers, including 25 of the Fortune 100 and more than 600 employees.

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. The CrowdStrike Falcon™ platform stops breaches by preventing and responding to all attacks type – both malware and malware-free. Only Crowdstrike unifies next-generation antivirus with EDR (endpoint detection and response), backed by 24/7 proactive threat hunting – all delivered via the cloud.

Nobody knows cyber-security like F-Secure. For three decades, F-Secure has driven innovations in cyber-security, defending tens of thousands of companies and millions of people. With unsurpassed experience in endpoint protection and response, F-Secure shields enterprises and consumers against everything from breaches to opportunistic ransomware infections to advanced cyber-attacks.

F-Secure's sophisticated threat intelligence combines the power of machine learning with the expertise of its world-renowned Labs for a singular approach called Live Security.

F-Secure's security experts have participated in more European cyber-crime scene investigations than any other company in the market, and its products are sold all over the world by over 200 operators and thousands of resellers.

IBM Security assists organisations to holistically protect their people, data, critical applications and cloud and mobile infrastructures. Our Security solutions help prevent, detect and respond to even the most sophisticated attacks and fraudulent activity in order to limit business disruption, loss of private data, and reputational damage to the brand. Powered by deep analytics and trusted IBM Security expertise, our robust portfolio of comprehensive, scalable industry-leading tools delivers unparalleled security intelligence with reduced complexity and lower maintenance costs. Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Malwarebytes is the next-gen cyber-security company that proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

EDITOR'S CHOICE

WINNER

No More Ransom – founding members Kaspersky, EC3, Dutch Police, Intel Security

Law enforcement and IT security companies have joined forces to disrupt cyber-criminal businesses with ransomware connections.

The "No More Ransom" website is an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre (EC3) and two cyber-security companies – Kaspersky Lab and Intel Security – with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.

The project also aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection. The more parties support this project, the better the results can be. This initiative is open to other public and private parties.

It's no secret that ransomware has become a huge problem for cyber-security over the last few years. It has become so widespread that it could easily be called an epidemic. The number of users attacked with ransomware is soaring, with 718,000 users hit between April 2015 and March 2016, an increase of 5.5 times compared to the same period in 2014 to 2015.

Police forces cannot fight cyber-crime and ransomware alone. Security researchers cannot do it without support from law enforcement agencies. Responsibility for the fight against ransomware requires a joing effort between the police, the justice department, Europol and IT security companies.

Together the group will do all it can to disrupt criminals' moneymaking schemes and return files to their rightful owners, without the latter having to pay loads of money.

For this award there are no finalists, just a single winner.

SPECIAL RECOGNITION AWARD

WINNER

Marcus Hutchins aka Malwaretech

Marcus Hutchins is lauded as the hero that very possibly may have saved the NHS and many other organisations around the world from the full effects of WannaCry.

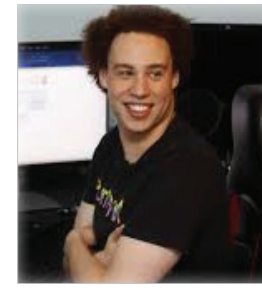
The 22-year-old slowed down the spread of the malware from his home on the North Devon coast. Known as MalwareTech on Twitter, Hutchins managed to register a garbled domain name hidden in the malware to track the virus, with the effect of halting the infection.

In a blog post, he described how he witnessed the outbreak of WannaCry and saw how the UK cyber-threat-sharing platform was flooded with posts about various NHS systems all across the country being hit.

He was able to get a sample of the malware with the help of Kafeine, a good friend and fellow researcher. He ran the sample through analysis and noticed it queried an unregistered domain, which he promptly registered.

The self-taught coder stressed that the registration of the domain was "not on a whim". He had registered several thousand such domains in the past year and then points them to a sinkhole server.

After the domain was registered, the spread of the ransomware was halted, preventing any further infection. Hutchins is now working with the government's National Cyber Security Centre to prevent any new strains of the ransomware.



For this award there are no finalists, just a single winner.

BEST ADVANCED PERSISTENT THREAT (APT) PROTECTION

WINNER

Carbon Black – Carbon Black Cb Defense

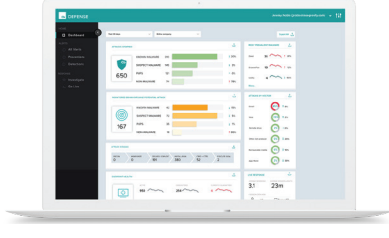
Cb Defense differs significantly from its competition because it focuses on preventing an attacker's behaviours and not simply blocking files. Competing products, specifically legacy AV and machine learning AV, detect malware at the moment of execution. Cb Defense focuses on more than just malware.

Cb Defense prevents non-malware attacks, which leverage a robust suite of tactics and techniques to penetrate systems and steal data. Traditional AV and machine-learning AV cannot see non-malware attacks. These competing solutions are designed to only identify threats at a single point in time – specifically, when a file is written to disk. Since they only look at the attributes of an executable file, they are completely blind in the face of attacks where no files are involved. This is precisely why Cb Defense was created.

Many customers use it to replace legacy AV, behavioural HIPS, network-based detonation engines, forensics solutions and file-integrity monitoring solutions, among others. Significant budget savings can be achieved replacing several products with one.

Cb Defense is virtually invisible to the user and rolls out in about 15 minutes. Security should not bog down a business from what it does day-to-day – something which Carbon Black kept in mind when creating and evolving Cb Defense. Security doesn't HAVE to be inconvenient.

Many organisations have very tight budgets. Recovering from a data breach is rarely a line item that's included. If using Cb Defense means that a business won't have to worry so much about the enormous cost of a data breach, they can meet and surpass budgetary expectations.



Finalists 2017

- Bromium for Bromium Secure Platform
- Carbon Black for Carbon Black Cb Defense
- Cylance for CYLANCEPROTECT®
- Fidelis Cybersecurity for Fidelis Enterprise
- Lastline for Lastline Enterprise
- TrapX Security for TrapX Deceptiongrid

BEST BEHAVIOUR ANALYTICS/ENTERPRISE THREAT DETECTION

WINNER

LightCyber/Palo Alto Networks – LightCyber Magna

The LightCyber Magna platform directly addresses the data breach crisis by quickly and accurately detecting external and internal attackers working towards a data breach. Currently, the industry average dwell time is five months, giving attackers healthy odds to successfully reach their objectives. Traditional security is simply not effective at detecting an active attacker working inside the perimeter, and it is almost certain that a motivated attacker will get into a network. As a reflection of its effectiveness and accuracy, it is shown able to uncover the activities of a simulated Red Team attack secretly being conducted.

Magna is easy to deploy and includes an agentless, on-demand endpoint capability that interrogates the endpoint for information to pinpoint an attacker or malicious activity. This also leads to fast remediation since the "smoking gun" has already been identified.

For confirmed alerts, the accuracy is 99 percent. The total number of alerts Magna creates each day is 1.1 per 1,000 endpoints on a network. This is reportedly orders of magnitude lower than typical security devices. LightCyber is believed to be the only company to publish its accuracy and efficiency metrics.

Magna has helped reduce personnel costs by enabling companies to avoid having to hire additional personnel. Magna may alleviate the need for a third-party scan and meets requirements for PCI DSS internal monitoring. Finally, companies such as law firms, that need to conduct security reviews, benefit from highlighting the capabilities of Magna, and they are likely to spend less time preparing for the review.

Finalists 2017

- Cisco for Cisco Stealthwatch
- CyberArk for CyberArk Privileged Threat Analytics
- LightCyber/Palo Alto Networks for LightCyber Magna
- NuData Security for Nudetect TM
- Securonix for Securonix Snypr Security Analytics Platform
- Vectra Networks for The Vectra Cybesecurity Platform
- ZoneFox for ZoneFox AI

BEST CLOUD COMPUTING SECURITY SOLUTION

WINNER

AlienVault – USM Anywhere

AlienVault's new USM Anywhere offers customers the same comprehensive, unified solution across cloud, hybrid cloud and on-premises environments. It is claimed to be the first all-in-one SaaS security monitoring platform designed to centralise threat detection, incident response and compliance management across these environments from a single, cloud-based console. USM Anywhere significantly reduces deployment time, so that companies of all sizes can go from installation to first insight within minutes.

USM Anywhere is the latest product to leverage AlienVault's proprietary, unified approach to security management. A cloud-based SaaS security monitoring platform, it combines the essential security capabilities needed for effective threat detection and response. Unlike other security solutions, USM Anywhere monitors cloud, hybrid cloud, and on-premises environments all from a single pane of glass.

SIEM installations are complex and expensive projects that often end up overshooting budgetary targets. The USM Anywhere platform enables organisations of all sizes to obtain the threat detection and remediation management that they need while still meeting budgetary expectations.

AlienVault is reportedly alone among vendors by integrating its SIEM engine with all other essential security controls. With USM Anywhere, customers don't have to purchase separate products or manage multiple consoles across cloud, hybrid and on-premises environments. Additionally, integrated threat intelligence provides the timely updates needed for effective threat detection and response. USM Anywhere's unified approach to security management provides customers with security visibility right out-of-the-box and exceptional value-for-money, as evidenced by its rapidly growing customer base.

Finalists 2017

- AlienVault for AlienVault USM Anywhere
- Bitdefender for Bitdefender Security for AWS
- Bitglass for Bitglass Cloud Access Security Broker (CASB)
- Boolebox for Boolebox Secure Sharing
- Skyhigh Networks for Skyhigh Security Intelligence Platform

BEST COMPUTER FORENSICS SOLUTION

WINNER

Guidance Software – EnCase Endpoint Investigator and EnCase Forensic

EnCase Forensic and EnCase Endpoint Investigator provide a powerful, judicially-accepted platform that serves as the foundation for corporations, government agencies and law enforcement to conduct digital investigations of any kind. Guidance knows the complexities of criminal investigations and what it takes to get to "case closed". Forensic is the trusted standard in criminal investigations and accepted in courts worldwide. Corporate investigators rely on Endpoint Investigator to complete more types of investigations than ever before. From HR issues, compliance violations, regulatory inquires, IP theft and others, it delivers full visibility across endpoints.

Forensic and Endpoint Investigator are designed based on feedback from thousands of investigators using the products, with innovations customised to speed examinations and increase efficiency. Powerful automation, distributed processing and advanced functionality create dramatic performance improvements and significantly reduce the costs associated with conducting investigations. Personnel do not need to travel to acquire data, nor do laptops or mobile devices need to be shipped for imaging.

Forensic is built with the investigator in mind, providing a wide range of capabilities that enables them to perform deep forensic analysis as well as fast triage analysis from the same solution. The solution enables investigators to quickly search, identify and prioritise potential evidence resulting in a decreased backlog.

Forensic acquires more evidence than other products on the market by collecting from a wide variety of operating and file systems, including mobile devices. This is the flexibility needed to ensure cases can be completed no matter where the potential evidence resides.

Finalists 2017

- Guidance Software for Encase Endpoint Investigator and Encase Forensic
- SolarWinds for MSP Risk Intelligence
- Forcepoint for Sureview Insider Threat
- Veriato for Veriato Investigator
- Unipart Cyber Security for ZDD Xnadata

BEST DATA LEAKAGE PREVENTION (DLP SOLUTION)

WINNER

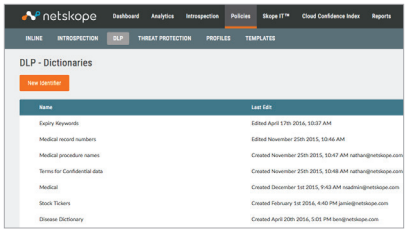
Netskope – Netskope Cloud DLP (integrated with the Netskope Active Platform)

The proliferation of cloud services has led to an exponential rise in the volume of sensitive business data stored in and shared across cloud environments. Netskope Cloud DLP enables IT to protect against intentional and unintentional data theft and loss across all SaaS, IaaS and PaaS solutions.

Through extensive data classification algorithms, heuristics and techniques, Cloud DLP isolates sensitive data and pairs it with contextual details specific to each transaction, including identity information such as user, location, device or browser, and user activity information such as share, upload/download or view. The platform aids IT in quickly identifying cloud service policy violations and trends in real-time, which further increases the accuracy of sensitive data detection and protection.

Unlike other DLP solutions, Netskope Cloud DLP is simple, flexible and easy-to-use. Enterprises can either define their own custom DLP profile or choose from industry-standard pre-defined profiles. It lets IT define DLP profiles and get policies up-and-running in minutes, while also providing powerful intelligence about real-time data loss in its environment – all within one simple workflow.

While traditional content inspection techniques often introduce too many false positives or negatives, Netskope Cloud DLP employs industry-first features, such as Exact Match capability, to provide surgical visibility into cloud service use and reduce false positives. It supports more than 3,000 data identifiers and 500 file types, plus keyword search, pattern matching and proximity analysis to increase accuracy. IT therefore requires less time to create the sensitive data policies necessary to mitigate security risks in real-time and reduce regulatory exposure.



Finalists 2017

- Forcepoint for AP-Data & AP-Endpoint
- Boolebox for Boolebox Secure Sharing
- Digital Guardina for Digital Guardian for DLP
- Netskope for Netskope Cloud DLP (Intergrated with the Netskope Active Platform)
- Cryptzone for Security Sheriff

BEST DISASTER RECOVERY/BUSINESS CONTINUITY OFFERING

WINNER

Druva

Druva provides a platform for data protection in the Cloud. Companies can protect critical business information that is created and stored within remote office servers, virtualised environments, cloud applications and laptops, tablets and phones.

More than 40 percent of company data exists outside the enterprise data centre. Data on laptops, phones, within cloud applications and in remote/branch offices is just as critical for disaster recovery/business continuity planning. Druva provides a comprehensive BC/DR platform for all company data, not just what's held in the data centre. Using Cloud, the cost for DR can be reduced by around 40 percent compared to traditional approaches.

Its cloud-based approach provides customers with a simple, scalable way to protect their data. By consolidating this data in the Cloud, companies can cut expenses on backup and disaster recovery.

This approach takes advantage of Druva's global deduplication, auto-tiering and micro-services for efficient use of storage to reduce costs. Druva can maintain comprehensive data security, comply with rapidly evolving global compliance and data privacy regulations. Companies can protect their data against attacks by using the Cloud as a platform for storing data.

Its approach provides support for multiple business continuity and disaster recovery uses without needing multiple copies of data. Stored data is instantly replicated across data centres within a region for redundancy. Using a special storage model, Druva creates a single golden dataset that can be repurposed to address multiple data protection needs.

Supporting multiple workloads on a common dataset significantly lowers each customer's total IT costs.

Finalists 2017

- Databarracks for Databarracks DRAAS
- Druva for Druva Platform
- Everbridge for Everbridge Platform
- Zerto for Zerto Virtual Replication

BEST EMAIL SECURITY SOLUTION

WINNER

Sophos – Sophos Email on Sophos Central

Sophos Email is a cloud-delivered secure email gateway engineered to keep businesses safe from email threats. It stops spam, phishing, malware and data loss and keeps employees productive. For SMEs that want to consolidate protection, it lets them control their email security alongside endpoint, mobile, web and wireless protection using Sophos Central's single interface.

Many organisations have moved to cloud email services. Deploying Sophos Email alongside a cloud email service adds an extra layer of email security and provides reassurance of email continuity in case of cloud service disruption to cloud services.

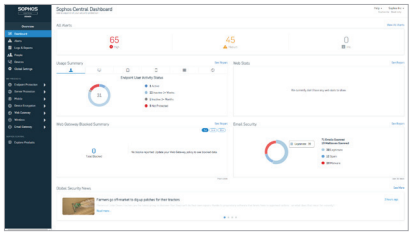
Sophos Email is a fully cloud-delivered solution and provides customers with a solution designed to be futureproof and can grow as their organisation grows. This means customers can reduce total cost of ownership because there is no need to over-provision hardware to anticipate future requirements.

Sophos Email provides the flexibility to meet the demands of changing infrastructure and user needs. Customers can effortlessly expand their cloud-managed security any time they require. It is infinitely scalable and update management is taken care of by Sophos in its SO2 compliant, globally-deployed, infrastructure.

The costs of maintaining legacy mail servers can quickly add up.

With Sophos Email's cloud gateway, costs are potentially reduced as there's no need to set up your own mail server, or manage and maintain gateway software.

The business receives a predictable monthly bill for added and deleted users, allowing users to scale as the demands of their business change. Updates are automatic and included in the subscription fee.



Finalists 2017

- Agari for Agari Enterprise Protect
- Libraesva Srl for Libra Esva
- Mimecast for Mimecast Targeted Threat Protection
- SonicWall for SonicWall Email Security
- Sophos for Sophos Email on Sophos Central

BEST FRAUD PREVENTION SOLUTION

WINNER

Proofpoint – Proofpoint Email Fraud Defense

Highly-targeted impostor email attacks, also known as business email compromise (BEC) scams, are one of the biggest threats to the enterprise today. The majority of these attacks spoof legitimate domains from trusted internal and third-party senders.

Proofpoint's Email Fraud Defense detects, blocks and responds to impostor email threats before they reach employees. Through a combination of strong email authentication (SPF, DKIM, DMARC), reputation and heuristics checks, Proofpoint stops email-based ransomware, prevents CEO/CFO wire transfer attacks and W2-scams, and blocks identity spoofing.

Combined with other Proofpoint Email Protection capabilities, its multi-layered approach empowers security teams to respond quickly and accurately to the most sophisticated threats.

As a cloud-based offering with a managed service offering, its solution is flexible and easy to use from day one, featuring a low total cost of ownership. Value is delivered immediately through threat detection and domain and mail stream discovery.

Today's cyber-crime is very focused on targeting users as opposed to systems. Proofpoint addresses this with solutions that protect people in the way that they work – meaning the ability to protect users on or off the corporate network, and on any device, that they may be using. It also protects the data that people are creating that is targeted by the attackers. And when something does go wrong, Proofpoint's solutions enable security staff to respond quickly.

By allowing customers to focus on their business and enabling their users to work the way they need, Proofpoint provides a sound business benefit for its customers by enabling them to strengthen their businesses.

Finalists 2017

- IBM for IBM Truster
- iovation for iovation Fraud Protection
- NuData Security for Nudetect
- Proofpoint for Proofpoint Email Fraud Defense
- Trusted Knight for Protector

BEST IDENTITY MANAGEMENT SOLUTION SPONSORED BY CROWDSTRIKE

WINNER

SailPoint – SailPoint Open Identity Management Platform

To help enterprises adapt to new security strategies and embrace a user-centric approach, SailPoint introduced the first Open Identity and Access Management Platform, believed to be the most comprehensive, end-to-end suite of on-premises and cloud-based (Identity-as-a-Service) solutions for compliance, provisioning, password management, single sign-on and managing structured and unstructured data.

SailPoint's Open Identity Management Platform gives users the identity context needed to make better-informed, real-time decisions to maintain secure access to an organisation's data, while enterprises are better positioned to manage processes and events across their infrastructure through more granular policy, controls and prioritised security alerts.

While identity is a growing threat to the enterprise, it is also a key business enabler. The balance between empowering users and protecting the business requires putting identity at the centre of how users – both employees or external – gain access.

SailPoint's Open Identity Management Platform empowers businesses to implement new technologies such as cloud and mobile, implement new business processes, collaborate with partners, vendors and other external users and open new business opportunities without the fear of exposing the organisation to undue risk as it relates to granting and managing access to sensitive data and applications.

In addition, it is designed to simplify IAM activities for end users. By delivering a simple and convenient user experience that is accessible from any device – laptop, desktop, tablet or mobile – users feel empowered to manage access without needing IT assistance.

Finalists 2017

- Centrify for Centrify Identity Service
- IBM for IBM Identity Cloud Service
- IBM for IBM Identity Governance and Intelligence
- Balabit and Lieberman Software for Integrated Privileged Access Management Platform
- Omada for Omada Identity Suite
- SailPoint for SailPoint's Open Identity Management Platform

BEST MANAGED SECURITY SERVICE

WINNER

IBM Managed Security Services

IBM is an industry-leading managed security services partner which can provide a high level of personalised protection from attacks, including in the cloud. IBM has differentiated itself from other managed security services providers by making significant investments in people, facilities, tools and cutting-edge cognitive technologies to provide its clients with a service built on industry-leading security intelligence and proven security methods delivered by security experts.

IBM has access to huge volumes of threat intelligence and real-world insights that can be used to create personalised protection from security threats.

With IBM MSS, IBM serves as a natural extension of a client's security team, providing the highest quality of service while addressing a client's specific security requirements.

IBM MSS integrates with a client's IT security team in their daily operations focused on detecting unwelcome events, managing incidents and reducing the risk to the customer's business, whether with an outsourced or a shared/co-sourced model, covering security monitoring or full management.

The service can be activated quickly, courtesy of 24/7 operations, with dedicated engineers and project managers, and it adheres to a mature set of quality assured processes that ensure the systems are implemented and the service activated in line with industry best practices.

Its customers benefit from early reduction in their exposure to threats and improves their security posture. The flexibility of its portfolio allows the selection of only needed components, with the option to adopt other, desirable services when the customer's business case stacks up to take advantage of IBM's extensive security portfolio.

Finalists 2017

- ECS for ECS Managed SOC Service
- IBM for IBM Security - Managed Security Services
- F-Secure for Protection Service for Business (PSB)
- Nettitude for Threat2Alert from Nettitude
- Zenedge for Zenedge Malicious Bot Detection Managed Security Services

BEST MOBILE SECURITY SOLUTION SPONSORED BY BOOLEBOX SECURE SHARING

WINNER

Wandera Secure Mobile Gateway

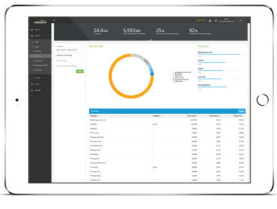
Mobile is the new frontier for cyber-threats. As adoption of corporate mobility continues to grow, so too does the number of attacks.

Wandera provides enterprise-grade threat defence against these mobile security risks, keeping devices secure across all four levels of protection as identified by Gartner including app scans, network security, device behavioural anomalies and vulnerability assessments.

Wandera also allows enterprises to prevent exposures by proactively limiting access to known risks and prevent problems before they arise. For example, adult sites, gambling apps and other content categories have been proven to be far more likely to leak data, employ unencrypted technologies and otherwise expose organisations to increased risk. Rogue or careless employees can also be stopped before uploading sensitive data on unsupervised file-sharing sites.

Unlike other mobile security approaches that are focused on one portion of the data journey , Wandera is the world's first cloud gateway for mobile that touches every point of the data journey. Wandera uses a unique multi-level architecture with three touch points: on the device, in the cloud and with the company's Enterprise Mobility Management (EMM) solution. This design enables billions of daily mobile data inputs to be scanned, creating the largest mobile dataset of information in the industry which ultimately powers a holistic and superior solution.

Wandera uses the latest techniques in AI and machine learning to analyse this data to surface insights and detect threats on a level we've never seen before. The company called this intelligence engine MI:RIAM. MI:RIAM has already found a number of zero-day vulnerabilities in the apps of huge brands like British Airways and Royal Mail.



Finalists 2017

- CipherCloud for Ciphercloud Mobile App
- F-Secure for Freedome for Business (FFB)
- IBM Security for IBM Security IBM MAAS360 UEM
- MobileIron for MobileIron Access
- Proofpoint for Proofpoint Mobile Defense
- Wandera for Secure Mobile Gateway

BEST MULTIFACTOR SOLUTION

WINNER

Yubico – YubiKey 4

Trillions of pounds are lost and billions of internet users risk getting their online accounts hacked because of compromised static credentials. YubiKey provides an additional layer of security beyond the password with the touch of a button.

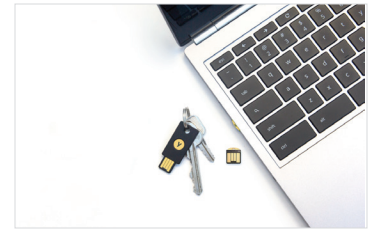
YubiKey 4 introduces an ease-of-use that has historically been a barrier to entry for large-scale adoption of strong user authentication, offering what is described as the most secure, easiest to use, and most economical method, with multi-protocol options that support legacy and emerging standards.

It cures the now painfully obvious password weakness in current access controls for applications and online services. The YubiKey 4 has options, such as public key cryptography and smart card support, that eliminate common attack vectors, such as phishing and man-in-the-middle exploits.

In 2016 Yubico launched a new service with Digidentity and the UK Government to secure its new GOV.UK Verify service for UK citizens accessing government services digitally – the first government service globally to offer secure identities using the open FIDO U2F standard co-created by Yubico.

The YubiKey has the lowest total fees and annual total cost per credential – without compromising on security, quality, usability or ethics. Last year, Google found the YubiKey was four times faster to log in, support calls were reduced by 40 percent and there were significant reductions in fraud attempts.

The one-time cost for the YubiKey significantly reduces ongoing licensing, acquisition and upgrade costs associated with other authentication solutions. The high security/ease-of-use of YubiKey 4 simplifies training for employees, eliminates the low security of SMS and time loss of typing a code to authenticate, and reduces support issues.



Finalists 2017

- CensorNet for CensorNet MFA
- Duo Security for Duo Security's Trusted Access Solution
- RCDevs for Openotp Enterprise MFA Server
- Gemalto for Safenet Authentication Service
- Yubico for Yubikey 4

BEST NAC SOLUTION

WINNER

ForeScout – ForeScout CounterACT

Enterprise networks contain a vast, increasing range of devices: computers, mobiles, industrial controls, VMs and other 'things'. Diversity accelerates hybrid IT environments, and IoT is becoming the norm. With increasing diversity, the complexity and confusion of security increases.

ForeScout has pioneered an agentless approach to network security, responding to the explosive growth of mobile computing and the IoT.

ForeScout CounterACT is a different type of network access control product, built for today's campus- and cloud-networks.

ForeScout offers a highly scalable, heterogeneous platform, providing enterprises and agencies with agentless visibility and control of devices and endpoints as they connect. Its technology continuously assesses, remediates and monitors devices, and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimise existing investments. As of 30 September 2016, more than 2,200 customers in over 60 countries improve their network security and compliance with ForeScout.

CounterACT can provide a significant improvement in the total cost of ownership (TCO) thanks to the ability to see and control devices and orchestrate information sharing and operation among a variety of tools. By integrating with leading network, security, mobility and IT management products, it enables significant savings.

Customers say they calculated the purchase and deployment costs of competitors' products to be multiple times that of CounterACT.

CounterACT also has what is believed to be the largest commercial NAC deployment in the industry in terms of endpoints deployed – one customer, a global financial services company, is monitoring over one million endpoints.

Finalists 2017

- Cryptzone for Appgate
- Cisco for Cisco Identity Services Engine
- Forescout for Counteract
- F5 Networks for F5 Networks Big IP
- Bradford Networks for Network Sentry

BEST SIEM/BEHAVIOURAL ANALYTICS TOOL

WINNER

Splunk – Splunk Enterprise Security 4.5 (ES) with Adaptive Response

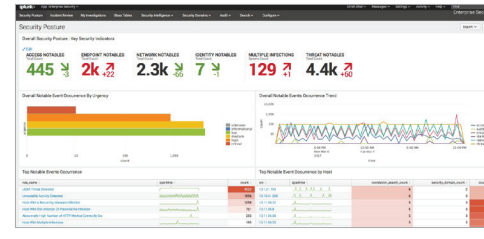
Advanced cyber adversaries are leveraging new attack methods that span multiple domains, launching devastating attacks that leave enterprises vulnerable. Despite advancements in security technologies, most solutions are not designed to work together or out of the box.

Splunk Enterprise Security 4.5 (ES) is a next-generation SIEM platform used by thousands of security customers for log management, continuous monitoring, incident investigation and response, security and compliance reporting, fraud detection, real-time correlation and detection of known/unknown threats. Splunk can index any type of machine or log data without the need for upfront normalisation at scale, so all data can be quickly indexed, searched, correlated, analysed, alerted, triaged, reported and tracked for security. Splunk's Adaptive Response provides connected intelligence for security operations to help organisations gain full visibility and responsiveness.

Business advantages include compliance with governance mandates, quick detection of advanced threats and malicious user activity using threat intelligence. Customers gain fast time-to-value because Splunk is a software-only, intuitive-to-use solution that contains pre-built functionality.

It can also be used for a wide range of IT operations and business use cases alongside security and compliance.

Technical advantages include scalable deployment on premises and in the cloud. APIs and SDKs can be leveraged to integrate Splunk into the broader infrastructure. The addition of new machine learning and data science models, new data source, and additional threat detection use cases advance the product's threat and anomaly detection capabilities further.



Finalists 2017

- AlienVault for AlienVault Unified Security Management (USM)
- IBM for IBM Security 0 IBM Qradar
- LogRhythm for LogRhythm Security Intelligence and Analytics Platform
- Splunk for Splunk Enterprise Security 4.5 (ES) with Adaptive Response
- Trustwave for Trustwave Managed SIEM

BEST UTM SOLUTION

WINNER

Sophos – Sophos XG Firewall

Sophos XG Firewall makes managing advanced protection simple by providing more defence in a single appliance than any other firewall. Sophos XG Firewall provides unprecedented visibility into your network, users and applications right from the control centre.

The Security Heartbeat pulses real-time information about suspicious behaviour or malicious activity between endpoints and the network firewall or UTM. By giving these products the ability to directly share intelligence, the Security Heartbeat can instantly trigger a response to stop or help control a malware outbreak or data breach.

Sophos is one of the only vendors that delivers on the original promise of Unified Threat Management, consolidating all the necessary network security solutions a modern organisation requires into a single appliance. It bills itself as the only UTM vendor that integrates Email encryption and DLP, a Web Application Firewall, and historical reporting into its UTM product along with all the other capabilities of a UTM. This dramatically reduces cost and complexity vs competitors and saves organisations significantly.

Sophos XG Firewall allows organisations to replace numerous other security solutions with a single appliance, helping to make budgets go much further and reducing the administrative effort for IT staff. Its streamlined user experience makes managing network security easier than ever.

Sophos products are intended to deliver the lowest total cost of ownership in the industry with aggressive pricing, the best hardware performance at every price point (proven in independent testing) and a focus on management simplicity that enables an IT generalist to easily deploy and manage its products. Upgrades and updates are automatic and included for the life of the product.

Finalists 2017

- 5nine Cloud Security for 5nine Cloud Security V9
- Cisco for Cisco Meraki MX
- SonicWall for SonicWall TZ Series Wireless Series
- Sophos for Sophos XG Firewall
- WatchGuard Technologies for WatchGuard Firebox T70

BEST VULNERABILITY MANAGEMENT SOLUTION

WINNER

Core Security – Core Impact/Vulnerability Insight

Core Vulnerability Insight allows customers to evolve their vulnerability management programme and improve their overall security posture. It offers greater scalability and advanced attack path analytics, to help users accurately identify the vulnerabilities that pose the greatest threat to critical business assets. It also allows for multiple vulnerability scans across vendors, while matching known exploits and simulating attacks, enabling customers to focus on the most vulnerable points of their network. Once critical vulnerabilities are prioritised, companies can move quickly to remediate the threat within their systems.

It provides a holistic view of an organisation's threat risk. It differs from other products with its use of attack path mapping. Through this attack path mapping, it reveals how adversaries can move multiple vulnerabilities across layers of infrastructure to reach and expose the most valuable assets.

The product allows customers to adjust which exploits and resulting attack paths are displayed on the risk they pose. This display highlights the most urgent attack paths and de-emphasises the lower priority paths, allowing security operatives to quickly modify attack path traits. After high-risk attack paths have been identified, ranked and eliminated, users can visualise and report the improved risk state.

It generates massive amounts of vulnerabilities as a result of both network and web scanning activities, making the need for vulnerability intelligence solutions essential. By consolidating multiple vulnerability scans across vendors, matching known exploits and simulating attacks, Core Vulnerability Insight provides a clear set of target systems based on the analytics it performs. This enables customers to focus on and remedy immediate vulnerabilities, ultimately saving them money.

Finalists 2017

- Core Security for Core Impact/Vulnerability Insight
- F-Secure for F-Secure Radar with Riddler Plug-in
- Rapid 7 for Rapid 7 Nexpose
- Tenable for SecurityCenter Continuous View ®
- Skybox Security for Skybox Vulnerability Control

BEST WEB CONTENT MANAGEMENT SOLUTION

WINNER

Sophos – Sophos Web Gateway

Organisations need comprehensive protection from the latest web threats. IT managers also need to be able to control web usage to ensure employee productivity.

The way users access the web has changed. They use multiple devices and cloud services and consume these anywhere, both in the office and remotely. IT teams need a solution that enforces policy and secures web browsing on all user devices, wherever they are.

Sophos Web Gateway provides cloud-delivered security reliably and effectively and enforces policy consistently to control web usage on PCs, Macs, Chromebooks and Apple devices. And along with web protection from Sophos Web Gateway, the full Sophos Central solution provides fully integrated web, email, endpoint, mobile and server protection managed from a single console.

Sophos Web Gateway is a fully cloud-delivered solution and provides customers with a solution that is designed to be futureproof and can grow with their organisation. It provides the flexibility to meet the demands of changing infrastructure and user needs. With minimum effort customers can expand their cloud-managed security any time they require. It is infinitely scalable and update management is taken care of by Sophos in its SO2 compliant, globally deployed infrastructure.

It actually enhances the end-user browsing experience and can speed up downloads. Sophos technology intelligently routes web traffic to the optimal gateway.

With no backhauling of remote user traffic to onsite hardware, customers get minimal latency with maximum security.

With Sophos Web Gateway, customers improve productivity and reduce help desk calls from unhappy users frustrated with slow browsing speed from competing solutions.

Finalists 2017

- Symantec for Blue Coat Secure Web Gateway
- Sophos for Sophos Web Gateway
- White Hat Security

BEST CUSTOMER SERVICE

WINNER

Barracuda Networks

Barracuda strives to provide fanatical and awesome customer service with live people always on the receiving end to help troubleshoot – there are no phone trees and no automated service.

Barracuda offers 24/7 phone-based technical support as part of the purchase price. Customers also can purchase additional options as part of an annual subscription.

With enhanced Barracuda Support, customers calling in are placed at the front of the queue. At the premium level, Barracuda will actively monitor the system and alert the customer if something goes wrong.

In addition, all customers can access a large support area via the website that includes a knowledge base, user forum, product documentation and other helpful resources.

Since inception, Barracuda has prided itself on the "IT Guy Next Door" mentality – making sure that there is always a live person available to help with any customer issues 24 hours a day, seven days a week.

Barracuda support is offered to every customer who provides a Barracuda serial number. Barracuda focuses on customer request, whether there is a valid subscription or not. All Barracuda's remote services and remote support is free of charge. Barracuda prides itself on a 99 percent customer renewal rate since inception, driven by exceptional service. It maintains a continuous feedback loop using in-person seminars, user groups, online customer feedback forums, regular customer surveys and ongoing communication and support. It leverages its channel partners, keeping its pricing model simple and affordable.

It develops solutions that are easy to use, easy deployment and an all-inclusive feature set.

Energize Updates keep products updated with the latest protection against threats.

Finalists 2017

- Avecto
- Barracuda Networks
- Ciphercloud
- Globalscape
- Proofpoint

BEST EMERGING TECHNOLOGY SPONSORED BY F-Secure

WINNER

High-Tech Bridge – ImmuniWeb

ImmuniWeb Web Security Testing Platform leverages a machine learning technology for intelligent automation of web vulnerability scanning. Complemented by human intelligence, it detects the most sophisticated vulnerabilities and contractually guarantees zero false-positives.

The first prototype of ImmuniWeb was launched in 2014 based on High-Tech Bridge's concept of hybrid security assessment that combined vulnerability scanning and manual penetration testing in real time. In 2015, Frost & Sullivan's Market Insight named ImmuniWeb "the most advanced hybrid on-demand web penetration testing".

At the beginning of 2016, ImmuniWeb vulnerability detection engine and almost all the algorithms were entirely revised and based on High-Tech Bridge's proprietary machine learning technology using Artificial Neural Networks (ANN). This emerging approach is leveraged for intelligent automation of vulnerability scanning and detection – ImmuniWeb is claimed to detect at least twice as many vulnerabilities than any automated solution would. It provides the same quality, reliability and comprehensibility as manual penetration testing, but in twice the time and at a more competitive price.

Its web security testing platform is based on High-Tech Bridge's proprietary machine learning ANN technology.

In an age where there is a shortage of cyber-security talents, ImmuniWeb's intelligent automation becomes increasingly important for companies looking for reliable and cost-efficient security solutions.

Its agility and 24/7 availability enables any individual and company to start application security testing in a few minutes from his or her mobile from any part of the world at any time. ImmuniWeb eliminates the routine of paper-based contractual approach.

Finalists 2017

- **High-Tech Bridge SA for ImmuniWeb®, Application Security Testing Platform**
- **Recorded Future for Recorded Future Intel Cards**
- **Sqrrl for Sqrrl**
- **IBM for Watson for Cyber Security**
- **ZoneFox for ZoneFox AI**

BEST ENTERPRISE SECURITY SOLUTION

WINNER

Cylance – CylancePROTECT

Complementing Cylance's revolutionary technology is a set of consulting services that provide pre-attack penetration and vulnerability testing, compromise assessments and post-attack incident response. Its experts organise information so customers can see their full security picture, and then offer strategic and tactical recommendations to ensure customers become secure.

When enterprises initially deploy CylancePROTECT, it is common to find active threats or evidence of previously unknown compromises. This quickly leads to the realisation that legacy antivirus solutions have left them vulnerable to numerous malware attacks, and that an overwhelming amount of work will be required to eliminate these threats.

This is where Cylance Consulting experts help organisations overcome challenges like partial installations, improper configurations, internal resource constraints, lack of training and the inability to maintain security optimisation. Its services expedite the implementation of CylancePROTECT, mitigate any risks that are identified and facilitate immediate ROI, bringing customers to a state of prevention.

In the face of constant innovation from attackers, many traditional antivirus vendors continue to focus on aging technologies that cannot keep up with the large numbers of new or mutated threats.

Traditional antivirus and endpoint security solutions routinely fail to detect even 50 percent of these threats, require constant network connectivity to provide protection and access frequent signature updates, consume vast system resources and are increasingly complex to deploy and manage.

Cylance products address these problems in a single solution that delivers measurably better enterprise endpoint security at an attractive, and often lower, total cost of ownership.

Finalists 2017

- **Cylance for CylancePROTECT**
- **Neustar for Neustar Siteprotect**
- **Skybox for Skybox Security Suite**
- **Symantec for Symantec DLP 14.5**
- **Whitehat Security for Whitehat Security Sentinel Platform**

BEST RISK MANAGEMENT/REGULATORY COMPLIANCE SOLUTION

WINNER

IRM Security – IRM SYNERGi

SYNERGi's growth has continued over the past year, with Unilever, BBC Worldwide, ASOS, Hutchinson 3G, Lloyds of London and Amadeus – alongside numerous small and medium-sized businesses – joining its customer base.

Despite only being in its fourth year of operation, SYNERGi now enables some 40 organisations to simplify cyber-security management, compliance, risk assessment and vendor management. This includes some of the UK's most trusted brands – names like the Post Office, Auto Trader, Debenhams and Deloitte.

But SYNERGi hasn't just grown by number of users. It's also progressively more involved with its existing customers, and many organisations are expanding the number of SYNERGi modules they use, bringing the platform into more areas of the business.

The fully managed, SaaS model SYNERGi includes no management costs or configuration or update constraints. Because its solution offers a modular approach, annual service and maintenance costs vary between roughly £25,000 per annum for one module up to £95,000 for those taking advantage of all six: governance, risk management, compliance management, audit management, vendor management and incident response.

This means SYNERGi can be configured and deployed on a case-by-case basis to align with a customer's needs and budgets – there's no need to buy anything they won't use. It actively encourages its customers only to invest in the modules that will deliver the most value to them in their current situation, and its consultative approach means it is on hand to talk them through the next steps as their needs grow.

IRM is constantly looking to improve, and its investment in the development of SYNERGi shows as much.

Finalists 2017

- IBM for IBM Resilient IRP Privacy Module
- IRM for IRM Synergi
- Netwrix for Netwrix Auditor
- SureCloud for SureCloud Platform for Risk Management and Compliance
- Forcepoint for Triton AP-Data
- TRUSTe for TRUSTe Assessment Manager

BEST SME SECURITY SOLUTION

WINNER

Proofpoint – Proofpoint Essentials

Proofpoint Essentials provides an extremely high level of follow-the-sun support with consistently high levels of customer service satisfaction scores. Global support 24/7/365 is included as part of the Proofpoint Essentials subscription with phone, email and live chat communication options.

The support team not only contributes to Proofpoint's ever expanding knowledge base but also to its library of technical videos that help both on-board new customers and provides existing customers a reference point on various product features should they need access.

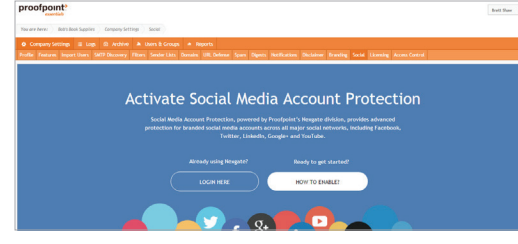
It is a user-friendly, cloud-based security service with a low total cost of ownership. All costs and management of the infrastructure and updates are included in the annual subscription. As an integrated offering, administrators can access all elements of email security, social media security and archive through a single portal.

Customers can be up and running in minutes with a simple, easy to navigate user interface, with multi-level logon options that make managing users a breeze. An intuitive end-user experience is designed to minimise the need for IT to act as a conduit for users to access their email quarantines, email continuity or archive. All end users can access these tools through easy-to-use web-based tools and integrations.

For MSP partners looking to migrate their customer base away from the other EOL solutions, Proofpoint offers an automated migration enabling them to move multiple customers with very little effort.

Small businesses are also targeted with the same threats as large enterprises, and Proofpoint Essentials protects SMEs from these threats.

Proofpoint Essentials helps SMEs secure their social media channels and protect their customers from malicious URLs and attachments posted by users.



Finalists 2017

- Bitdefender for Bitdefender Gravity Zone
- Foregenix for FGX-Web
- Netwrix Corporation for Netwrix Auditor
- Proofpoint for Proofpoint Essentials
- WatchGuard Technologies for WatchGuard Firebox M300

BEST NEWCOMER SECURITY COMPANY OF THE YEAR

WINNER

Aqua Security

Virtual containers are rapidly being adopted in enterprise deployments, but they present particular security challenges due to the scale, agility and open nature of the container operating environment. The rapid DevOps process that is often behind container deployments and the inclusion of many open source components require tight governance of the process from the development phase and beyond.

Aqua's Container Security Platform was purpose-built to address the container-specific security challenges. It provides visibility into container activity and the ability to isolate containers from each other, protect kernel integrity, maintain granular user and network access controls and deliver automated intrusion detection and intrusion prevention in container environments while remaining transparent and non-intrusive to developers.

Aqua enables organisations to reap the business benefits of containers without increasing their risk profile, plus harness the power of automation to reinvent application security – more effectively and efficiently.

Software containers are experiencing extremely rapid adoption. Especially in large enterprises with mature security organisations, Aqua has seen container initiatives stalled due to security concerns. By providing a comprehensive platform for securing containerised environments, Aqua enables its customers to extract all the cost, agility and efficiency benefits containers offer without increasing their risk profile.

By enabling its customers to use automation to "bake security into" container application development (or in DevOps speak, to facilitate security's "left shift"), Aqua enables organisations to inherently improve their application security posture. With Aqua, the next generation of container-based applications will be more secure and have better structural integrity than ever before.

Finalists 2017

- Aqua Security
- Coronet
- Redscan Cyber Security LTD
- Vectra Networks
- Verint Threat Protection System

BEST SECURITY COMPANY

WINNER

Symantec

Symantec is the largest cyber-security company in the world, helping consumers, small businesses and the world's leading enterprises secure and manage their data. The company counts 90 percent of the Fortune 500 as customers of its SSL certificates, and has the largest market share (31.5 percent) and protection capabilities in endpoint protection. Symantec is also the leading email security provider with 20.9 percent market share according to IDC and scans 30 percent of the world's enterprise email traffic each day. Nearly a third of the company's revenue comes from the EMEA region.

Moreover, the 2016 acquisitions of Lifelock and Blue Coat in 2016, brought another 4.4 million highly-satisfied customers and 5,000 organisations – including more than 70 percent of the Fortune Global 500 – into the Symantec fold. Significant continued customer growth is expected.

Symantec invests more than $US 1.1 billion (£860 million) every year in security R&D, and it increased the budget this year, particularly in areas such as URSA, its Information Protection division (in which its DLP product grew its market share by 37 percent last quarter), and IoT (Symantec is already securing more than 1 billion IoT devices worldwide).

Unified Risk and Security Analytics (URSA) allows Symantec to feed information to its products and services to provide customers with the latest security intelligence. The combination of Symantec and Blue Coat puts the company at the bleeding edge of using AI and machine learning for cyber-security innovation. Specifically, it enables the training of the world's most advanced security by the world's largest civilian intelligence network.

The acquisition also brings together a formidable scale of investment in R&D and threat research.

Finalists 2017

- Crowdstrike
- Cylance
- Egress Software Technologies
- IBM
- Malwarebytes
- Symantec

BEST PROFESSIONAL TRAINING OR CERTIFICATION PROGRAMME

WINNER

PhishMe – PhishMe Simulator and Reporter

The PhishMe methodology turns every employee into an IT security-aware professional, transforming a company's biggest liability into its strongest security asset. The behavioural conditioning methods prepare employees to recognise and resist malicious phishing attempts. Employees are conditioned not only to identify and report phishing attempts but also to provide critical attack intelligence to the IT security teams in defending against data breaches, ransoms and system shutdowns.

PhishMe users are further developing and strengthening a bank of real-world threat information which helps IT security managers to better defend their organisations against threats. The real-time visibility on attacks bolsters professionals' knowledge of the threats their organisations are facing. This information is of course tailored to their company and industry as it's based on up-to-the-minute attempts to breach that company.

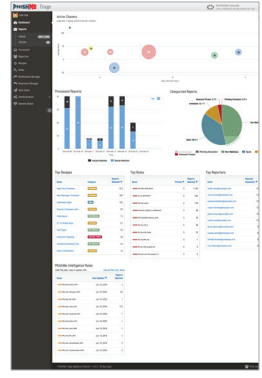
PhishMe analysts and researchers work to analyse and verify the plethora of phishing threats and provide real-world training simulations that prepare customers for actual attacks. The enhancements enable IT security professionals to create a wider range of the latest threat scenarios to test employees.

Employees are conditioned to recognise and report malicious phishing emails into the PhishMe Simulator which provides ongoing support for the IT professional through deep metrics, benchmarking and reporting options.

Following this step, customers can streamline the intelligence generated into the PhishMe Reporter, a next-generation threat management and incident response platform which provides real-time visibility and fast verification of actual attacks in progress.

Finalists 2017

- (ISC)² CCSP
- (ISC)² CISSP
- (ISC)² SSCP
- ISACA for Certified Information Security Manager (CISM)
- Certification
- PhishMe for PhishMe Simulator and Reporter



BEST CYBER-SECURITY EDUCATION PROGRAMME

SPONSORED BY Malwarebytes

WINNER

The Information Security Group (ISG) at Royal Holloway University of London (RHUL)

The Information Security Group (ISG) at Royal Holloway, University of London, is a world-leading interdisciplinary research group dedicated to research and education in information (cyber) security. It has been recognised by EPSRC and GCHQ as one of eight Academic Centres of Excellence in Cyber Security Research in the UK.

The ISG contains more than fifteen full-time academic faculty members, including a mixture of computer scientists, mathematicians and social scientists that are supported by several research assistants and many research students, making the ISG one of the largest academic information security teams in the world. The group has expertise in cryptanalysis, combinatorial cryptography, provable security and message authentication codes.

The ISG was formed in 1990 with the intent of providing an academic institution which understood and collaborated with government and industry in information security.

The ISG retains its close links with industry, through collaborations with industry security professionals, a strong history of consultancy and an extensive international MSc alumni community.

The ISG also conducts research into socio-technical and organisational aspects of information security, two broad and rapidly expanding disciplines that include many topics of crucial importance to the science of cyber-security.

The research of the ISG has a strong focus on the security of systems and technologies, including the foundations of trust and security and the development of secure, large-scale applications and systems .

Finalists 2017

- Cyber Security Challenge Schools Programme
- Open University Online MOOC (MASS Open Online Course) Introduction to Cyber Security
- The Information Security Group (ISG) at Royal Holloway University of London (RHUL)

BEST SECURITY TEAM SPONSORED BY Carbon Black.

WINNER
Camelot

The team at Camelot has been re-built over the past 24 months. It started from humble beginnings with a security team of just two people following the departure, over the preceding three-month period, of the rest of the team.

The first 12 months was tough for the team as it had to both maintain business as usual whilst recruiting. With no handover and little documentation, it also had to develop an understanding of the business, reverse engineer the architecture and configuration of the security technologies in place and build relationships with stakeholders.

Despite the challenges, the team delivered. In the summer of 2015 it developed a three-year infosec strategy which is now over halfway through successful execution, delivering ahead of schedule. Gartner maturity reviews in April 2015 and August 2016 showed improvements across all 10 metrics as well as tracking consistently above the retail sector average.

Twenty-four months ago, the team was an operational function in IT with a manager. Building a credible function and demonstrating the importance of infosec to the business meant that the head of the function was first put on the IT leadership team and then as a CISO on the business leadership team.

Over the past 12 months, the CISO has become a regular attendee at key business meetings, providing a platform to influence business decisions and wider business strategy. These include UK leadership team meetings, programme steering group meetings and the audit, risk and security committee.

Outside of Camelot the CISO has contributed to standard setting, public speaking at security conferences and the establishment of industry threat intelligence sharing groups.

Finalists 2017
- Camelot
- Canon Europe
- Skyscanner

CSO/CISO OF THE YEAR SPONSORED BY IBM

WINNER
Ed Tucker, HMRC

Ed Tucker has been working in IT and Security for more than 15 years. He currently leads HM Revenues and Customer's Cyber Security and Response capability, looking into areas such as Online Fraud, Hacking Analysis & Capability Scoring, Forensic Investigations, Cyber Threat.

Previously, Tucker was service security manager at Fujitsu Services on contract to HMRC.

The HMRC is probably one of the most phished brands in the world, most commonly with the classic 'Tax Refund Notification'.

Tucker has been working hard to implement security controls across all HMRC's email domains and has managed to reduce phishing emails by 300 million this year through spearheading the use of DMARC (Domain-based Message Authentication, Reporting and Conformance). This has enabled the organisation email service providers to identify fraudulent emails purporting to be from genuine HMRC domains and prevent their delivery to customers.

In the first six months of 2016, its dedicated Customer Protection Team responded to more than 300,000 phishing referrals from customers and instigated the takedown of more than 14,000 fraudulent websites.

The issue of protecting its customers from cybercrime will become even more important for HMRC in the years ahead as it increases its reliance on digital communications as part of the Making Tax Digital initiative.

The National Cyber Security Centre is heavily pushing DMARC adoption across the UK with Tucker having put HMRC at the forefront of that movement.

Finalists 2017
- Ed Tucker, Head of Cyber Security, HMRC
- Michele Hanson, CISO, Transport for London
- Phil Cracknell, CISO, HomeServe

SC 2017 awards
EUROPE

Haymarket Media Group
Bridge House
69 London Road
Twickenham
TWI 3SP

Telephone: +44 (0)20 8267 8016
Web: www.scmagazineuk.com