Tuesday, 5th June 2018
London Marriott Hotel
Grosvenor Square, Mayfair, London
W1K 6JP
### ABOUT ONETRUST

OneTrust is a global leader in enterprise privacy management software used by more than 1,500 organisations to comply with data privacy regulations across sectors and jurisdictions, including the EU GDPR. Our comprehensive and integrated platform includes readiness assessments, privacy impact assessments (PIA/DPIA) and data mapping automation, website scanning and cookie compliance, subject rights and consent management, incident reporting, and vendor risk management.

---

## ENTERPRISE PRIVACY MANAGEMENT SOFTWARE FOR GDPR COMPLIANCE

### READINESS & ACCOUNTABILITY TOOL

Benchmark organisational readiness and provide executive-level visibility with detailed reports.

- GDPR Articles 5 & 24

### PRIVACY ASSESSMENT AUTOMATION

Choose from pre-defined screening questionnaires to generate appropriate record keeping requirements.

- GDPR Articles 25, 35 & 36

### DATA MAPPING AUTOMATION

Populate the data flow inventory through questionnaires, scanning technologies or through bulk import.

- GDPR Articles 6, 30 & 32

### COOKIE CONSENT & WEBSITE SCANNING

Conduct ongoing scans of websites and generate cookie banners and notices.

- GDPR Articles 7 & 21 ePrivacy Directive Draft Regulation

### SUBJECT ACCESS RIGHTS PORTAL

Capture and fulfill data subject requests based on regulation specific requirements.

- GDPR Articles 12 - 21

### CONSENT & PREFERENCE MANAGEMENT

Track consent transactions, enable data subjects to manage preferences, and maintain records of consent.

- GDPR Article 7

### VENDOR RISK MANAGEMENT

Conduct vendor risk assessments, audit and manage data transfers to third parties.

- GDPR Articles 24, 28, 29 & 46

### INCIDENT & BREACH MANAGEMENT

Build a systematic process to document incidents and determine necessity for notifications.

- GDPR Articles 33 & 34

---

**ONLINE DEMO AND FREE TRIAL**

AT ONE TRUST.COM

INFO@ONETRUST.COM

ATLANTA | LONDON | MUNICH | BANGALORE
Recognising excellence

SC Media UK is once again delighted to honour and celebrate the achievements of those luminaries of our industry who, in the opinion of our judges, have stood out as exemplars in their chosen disciplines.

Each year our judges are astounded by the quality of the entries - yet it should not be so surprising. We are talking about an industry that employs some of the brightest minds on earth, tackling many of the most complex problems faced by humanity, working at the cutting edge of technology, often way beyond anything made public - whether that be in quantum computing, encryption, big data or artificial intelligence.

And in the wake of global attacks and new vulnerabilities, from WannaCry and NotPetya to Meltdown and Spectre, and the overtaking of physical crime with cyber-crime in many areas - cyber-security has rapidly risen up the agenda of boardrooms and governments, resulting in increased spend, translating as increased investment in research and development.

Then add well resourced and innovative adversaries in the mix, it makes the sector both challenging and exciting - if you can call being under attack exciting. It means we have had a plethora of innovative products and services from new and old players alike. But it also means they have faced tough competition to outdo each other and stand out from the competition. And while there are new threats needing inventive approaches to prevent or mitigate attacks, the old ones haven’t gone away, and more advanced versions tackle this increased complexity.

The result is that there are some great organisations doing excellent work who did not make it onto our shortlists. And there are truly brilliant solutions just pipped to the post for the top position in this particular race. But it also means that even if you don’t agree with every decision made by our judges, all our winners are truly world class and thoroughly worthy of praise.

So to those of you who made it onto the following pages - Congratulations!

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

Prof Richard Benham
Chairman, www.thecyberclub.org

Dr Achim D. Brucker
senior lecturer (system & software assurance), Sheffield University

Tony Collings
chairman, ECA Group

Martyn Croft
commentator/speaker, the use of technology and the role of information security in the charity sector

Jane Frankland
founder, Cyber Security Capital and The IN Security Movement

Prof. Steven Furnell
professor of information security, Plymouth University

Neira Jones
MD, Phoenix Edge

Tim Lansdale
head of payment security, WorldPay

Mike Loginov
CEO/CISO, AscotBarclay

Paul Midian
chief information security officer, Dixons Carphone

Sue Milton
board advisor, ISACA

Dr Steven Murdoch
principal research fellow, University College London

Troels Oerting
non executive director, board chair, Barclays Bank

Emma Philpott
managing director, Wyche Innovation Centre

Talal Rajab
head of programme cyber and national security, Tech UK

Pamela Rustem
member of the board, ISSA UK

Peter Shorney
global head of information security, Rentokill Iniital

Brian Shorten
chairman, Charities Security Forum

Howard Skidmore
head of information security and cyber, Crowe Horwath

Quentyn Taylor
director of EMEA information security, Canon-Europe

Dr Ismini Vassiliou
lecturer and programme lead, BSc (Hons) digital and technology solutions, The Univ. of Plymouth

Paul Watts
CISO, Domino Pizza Group

Elisabetta Zaccaria
chairman, Secure Chorus Ltd
SC Media UK thanks all sponsors for their generous support of the 2018 SC Awards Europe. This event, which helps raise professional standards in the information security industry worldwide, was made possible thanks to their involvement.

AlienVault® has simplified the way organizations detect and respond to today’s ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management®, with the power of AlienVault’s Open Threat Exchange®, the world’s largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource constrained IT teams.

Carbon Black has designed the most complete next-gen endpoint security platform, enabling organization to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations 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.

Duo helps defend organisations against breaches through its easy and effective cloud-based Trusted Access product suite. The company verifies the identity of users, and the health of their devices, before granting them access to applications. Duo’s balance of security and usability has led them to be an enduring and trusted partner to thousands of customers worldwide, including Etsy, University of York, Random House, Nibe, Betsson, Paramount Pictures, and more.

ForeScout Technologies offers the unique ability to see devices the instant they connect to the network, control them and orchestrate information sharing and threat response among disparate security tools. Learn how at www.forescout.com.

Gemalto (Euronext NL0000400653 GTO) is the global leader in digital security, with 2017 annual revenues of €3 billion and customers in over 180 countries. We bring trust to an increasingly connected world. From secure software to biometrics and encryption, our technologies and services enable businesses and governments to authenticate identities and protect data so they stay safe and enable services in personal devices, connected objects, the cloud and in between.

IBM Security, with 8,000 professionals in 133 countries, delivers an immune system of security technology to detect and prevent threats and respond quickly and completely to breaches. We address the evolving security landscape and our clients’ most critical needs with AI innovation in the cloud and intelligent orchestration. For more information, please visit www.ibm.com/security, follow @ IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

OneTrust’s privacy management software is used by more than 1,500 organizations to comply with data privacy regulations across sectors and jurisdictions, including the EU GDPR and ePrivacy (Cookie Law). The multi-lingual software is deployed in an EU cloud or on-premise, and is based on a combination of intelligent scanning, regulator guidance-based questionnaires, and automated workflows used together to automatically generate the record keeping required for an organization to demonstrate compliance to regulators and auditors.
Best Advanced Persistent Threat (APT) Protection

**WINNER**
Verint Threat Protection System

Siloed detection and investigation tools, multiple, unprioritised alerts and insufficient automation exacerbated by cyberskills shortage make it difficult to fully detect, understand, and remediate cyberattacks quickly. Many attacks go undetected for months.

Verint Threat Protection System, the first unified, pre-integrated intelligence-driven, augmented security platform, detects breaches across the attack chain. Through the power of automation, AI, and machine learning, it analyses thousands of leads daily, transforming them into a handful of prioritised incidents. It provides clear, visual storylines slashing discovery and investigation time, investigation, and forensics. The system establishes a recommended remediation plan for orchestrating the best response.

The solution monitors endpoints and networks to detect threats across the cyber-attack kill chain, relentlessly hunting attackers, gathering evidence, generating intelligence, and providing insights that stop cyberattacks. Because it rapidly processes knowledge to deliver Actionable Intelligence, it evolves quickly, recognising new types of attacks well before traditional perimeter systems can prevent them.

3D architecture with complete automation and orchestration provides visibility and protection across multiple attack surfaces: networks, endpoints, and payloads. Integrated functionality provides all critical cybersecurity capabilities - detection, prioritisation, investigation, remediation - in a single pre-integrated platform leveraging machine learning, AI, and augmented security.

The judges thought that this was a robust entry showing a highly competent product and in addition to providing the required basic features, it also uses augmentation, which is impressive and extremely beneficial for analysts.

Best Authentication Technology

**WINNER**
SecureAuth + Core Security

SecureAuth has developed an effective and flexible solution that ensures every identity authenticating is known and verified from sign-in to log-off. SecureAuth uses techniques that can check something they have (e.g. a device), something they know (e.g. knowledge-based questions) and something they are (e.g. biometric) creating infinitely customisable authentication workflows, protecting against attacks, while providing unparalleled choice.

Unlike others, SecureAuth offers the broadest set of authentication methods and what is believed to be more risk-based adaptive authentication than any other competitor. Here, it inspects the device the login is coming from, IP address, location, phone number, biometrics and behaviour analytics to determine a risk score without burdening the user. Depending on the risk score, it can either accept, step-up, redirect or deny the access attempt. Because it collects such rich threat data during authentication, it can share with a SIEM system or security operations centre (SOC) to help cut through a sea of network and endpoint alerts to decrease threat detection time.

Also unlike other vendors, SecureAuth can create infinite different authentication workflows for users or assets being accessed. This provides significant value in allowing the proper granularity to control consumers, workforce, partners and administrative users’ access from a single platform but in varying manners. SecureAuth is competitively priced compared to other vendors. SecureAuth IdP’s SSO improves user productivity.

According to judges, SecureAuth has developed an effective and flexible solution that ensures every identity authentication is known and verified from sign-in to log-off using techniques to check a device, knowledge-based questions and biometric.

---

Finalists 2018

- **Highly Commended**: Fidelis Cybersecurity
- Bitdefender Gravity Zone Elite
- CrowdStrike Falcon
- Lastline Enterprise Best APT Protection entry
- Proofpoint Targeted Attack Protection
- Sophos Intercept X
- Verint Threat Protection System

---

Finalists 2018

- **Highly Commended**: OneLogin
- Duo Security
- Ping Identity Platform
- SafeNet Trusted Access
- SecureAuth + Core Security
- VASCO
Zero Trust. Complete Confidence.

**TRUSTED USERS**
Make sure everyone is who they say they are.

Verify your users’ identities with two-factor authentication and enforce user access policies to ensure secure access to your applications.

**TRUSTED DEVICES**
Ensure their devices meet your standards.

Duo’s platform checks the security health of your users’ devices. Using our device access policies, you can block, warn or notify users of risky devices.

**EVERY APPLICATION**
Allow access to only the applications you deem appropriate.

Protect applications no matter where they’re hosted, including on-premises and cloud-based, and simplify access with our secure single sign-on.

Start your free 30-day trial at duo.com.
**BEST BEHAVIOUR ANALYTICS/ENTERPRISE THREAT DETECTION**

**WINNER**

**Exabeam Advanced Analytics**

Exabeam pairs automated threat detection with rapid search and investigation technology. Its proprietary Session Data model automatically stitches together user activities into timelines. These are used to baseline normal behaviour and identify anomalous activity. This allows analysts to tackle the often-labour-intensive task of tracking lateral movement across IP addresses, devices and credentials. Exabeam also automatically constructs timelines for all incidents discovered, thus automating much of the manual work analysts perform. Tasks that typically take days or weeks can be accomplished in seconds or minutes.

Exabeam also uses machine learning driven behavioural modelling, instead of correlation rules, to understand behaviour for every entity. The benefits include lower false positives, better detection or unknown attacks, less maintenance.

Exabeam also uniquely displays analysis of good behaviour alongside bad, to provide context. This helps analysts more quickly identify and triage threats. Unlike competitors, Exabeam’s point-and-click UI means even junior staff in the SOC can create very complex searches and instead of returning a single attack log, Exabeam returns an intuitive, pre-built timeline of the whole session involved in the incident.

SIEM vendors have attempted to compete in the behaviour analytics space. This model provides stability and predictability compared to SIEM. Since most customers have predictable growth they charge customers by the amount of data they store. Its subscription model offers predictable licensing fees.

The judges thought Exabeam Advanced Analytics was not just a great looking and fully functional product but also a great entry answering all of the questions and presenting real world cases where customers have benefitted.

---

**BEST CLOUD COMPUTING SECURITY SOLUTION**

**WINNER**

**AlienVault USM Anywhere**

AlienVault USM Anywhere enables organisations with limited resources, expertise, and budgets to benefit from the latest, cutting-edge security technologies. It’s the industry’s first all-in-one SaaS security monitoring platform that centralises and simplifies threat detection, incident response, and compliance management across cloud and on-premises environments.

USM Anywhere combines essential security technologies—asset discovery, vulnerability assessment, intrusion detection (network, host, and cloud), incident response, SIEM, log management and reporting—in one unified platform, alleviating the time and cost of purchasing, integrating, and managing a myriad of point security products.

Managed through a single pane of glass, USM Anywhere streamlines the process of detecting, prioritising, and responding to threats across cloud and on-premises environments. Designed with the needs of today’s resource-constrained IT security teams in mind, USM Anywhere reduces the time and budget required for effective security monitoring and compliance management.

USM Anywhere enables organisations of all sizes, especially those with smaller IT security teams, to obtain the threat detection and response management they need while still meeting budgetary expectations. At an affordable price, USM Anywhere provides an unified approach for simplified deployment, essential security controls, and integrated threat intelligence, maximising value.

According to judges, this is an effective, all-in-one solution that particularly suits organisations with a resource-constrained IT security team. The blend of lab-based and community-based threat intelligence data delivers continuous threat intelligence data which is triaged by the service instead of the in-house security team; a big plus.

---

**Finalists 2018**

- ** Highly Commended:** Varonis Data Security Platform
- ** Exabeam Advanced Analytics**
- ** Forcepoint UEBA**
- ** Splunk User Behavior Analytics**
- ** ZoneFox**

---

**Finalists 2018**

- ** Highly Commended:** Alert Logic Cloud Defender, Proofpoint SaaS Protection
- ** AlienVault USM Anywhere**
- ** Forcepoint CASB**
- ** My1Login**
- ** Vormetric Transparent Encryption by Thales, now with Live Data Transformation and Container Security**
One Giant Leap for Security
80% Faster Threat Detection and Response!

AlienVault® USM Anywhere™ is a unified security monitoring platform for early threat detection, rapid incident response, and simplified compliance management across cloud and on-premises environments.

According to a recent commissioned study by Forrester Consulting, USM Anywhere can help IT security teams improve threat detection and response times by 80% and save 2,000 hours per audit, delivering a 6x ROI over 3 years.

Discover why 7000+ organizations worldwide trust AlienVault USM for their security and compliance needs.

AlienVault.com/InfoSec2018

Redscan provides managed security services that protect organisations against cyber-crime. It applies its offensive security expertise to deliver market-leading managed detection and incident response services, red team operations, penetration testing, and security consulting services.

Redscan ThreatDetect is a 24/7 managed detection and response (MDR) service that identifies and contains cyber threats before they can impact business.

The service operates as an extension of an in-house IT team by integrating security experts, who have both offensive and defensive security knowledge, with best-in-class signature, behavioural and anomaly detection technology, threat intelligence, and forensic investigation tools to proactively hunt, detect and respond to cyber threats in real-time.

Whether organisations want to monitor their in-house applications and infrastructure, their cloud platforms and applications, or the end-points that connect to your critical information, ThreatDetect will ensure that threats are rapidly detected and responded to. The service can also be used to assist in adhering with a range of compliance obligations which include SWIFT, PCI, and ISO.

Working as an extension of clients’ in-house teams, Redscan’s security experts are always on-hand to provide support when needed. Where additional support (beyond any professional service hours and online & telephone remediation support included as part of the managed service), is requested, the company is able to provide, as an optional service, remote and/or onsite assistance.

Redscan strives to make the deployment process as swift and hassle-free as possible. SME deployment takes 2-3 days.

According to judges, the testimonials speak well of the service that the individuals are “willing to be fully on-record to this degree”.

Best Data Leakage Prevention (DLP) Solution

Winner

Code42 Security Center

First-generation DLP solutions prevented inadvertent loss of sensitive data from being transferred outside the corporate network. The current generation is evolving fast to prevent data loss from insider threats and malicious external attacks.

Consequently, there’s an increased focus on protecting endpoint devices, which hold 60 per cent of all enterprise data today. If you can’t monitor and protect endpoint data, you don’t have a complete DLP strategy in 2018. To help organisations with endpoint data, Code42 offers the following next generation protection services: for insider threats, Code42 monitors the movements of data on endpoints and alerts IT teams of suspect activity, detecting insider threats in minutes or hours, versus weeks or months compared to alternatives.

Code42 backs up every endpoint, every 15 minutes, or 96 times a day. When data loss, theft or breach happens, IT teams can restore devices on average within 30 minutes, dramatically reducing costs of lost productivity.

It supports user preferences by protecting data with a consistent experience across Mac, Windows and Linux. With continuous endpoint backups and customisable CPU settings, Code42 works silently in the background, so your users stay productive both on and off the corporate network – No VPN required.

Code42 is designed to scale from one user to hundreds of thousands with no impact on performance. Whether organisations choose cloud or on-premise, customisable installers make deployment fast and simple – days, not months.

A single IT admin can manage more than 100,000 users via the Code42 console. Configure, deploy, monitor and report on everything including, device backup and restore status.

Judges thought the product was a convincing solution with a great range of usability, easy scalable and system agnostic.

Finalists 2018

• Highly Commended: Flashpoint
• Avecto
• Barracuda Networks
• Mobliciti
• Proofpoint
• Redscan

Finalists 2018

• Highly Commended: Endpoint Protector
• Bitglass - DLP for the Cloud & Mobile Era
• Code42 Security Center
• Digital Guardian Data Protection Platform
• Forcepoint DLP
• Proofpoint Information Protection Platform
BEST DECEPTION TECHNOLOGY

WINNER
TrapX Security
DeceptionGrid

DeceptionGrid is used to bait, engage, and ultimately trap hackers that have penetrated a network. Deception enhances visibility and helps identify attackers that have bypassed all other cyber defences. Deception fills your network with lures (tokens) and decoys (traps) to deceive and detect hackers within the network. Deception surrounds the attackers with tempting targets. Everywhere they turn, they face immediate identification.

Tokens are fake credentials and scripts that are placed within your real information technology assets. These tokens appear to be exactly what attackers seek - information about valuable resources, credentials, and authentication to escalate permissions - and can include cached credentials, database connections, network shares, and much more. Attackers find this bait attractive and then these fake credentials and fake information lead them directly into a trap.

DeceptionGrid advanced Traps take the illusion much further. Families of specialised traps can present highly attractive targets for attackers and their specialised malware tools. These specialised emulated traps include networking equipment, telephony, internet of things (IoT) and embedded processor devices. Examples include medical printers, cameras, environmental controls and industry specific equipment such as ATM’s, Point of Sale (PoS) servers and terminals, medical devices, manufacturing PLM and SCADA components, and many others.

Detection methodology is simple and absolute - one touch of a trap will set off a high confidence alert. Alerts are high accuracy that detect attack unseen by other cyber defence.

Alternate technologies spend many CPU resources filtering traffic, trying to match signatures or guess at signatures.

According to judges, this product has a really good depth of the use of lures.

BEST EMAIL SECURITY SOLUTION

WINNER
FireEye Email Solution

Email is the highest volume data ingress point, making it the most vulnerable vector for cyber-attacks. FireEye Email Security catches traditional, mass email, phishing attacks with known malicious attachments, links and content, and emerging and targeted attacks as they occur. Emails are analysed for threats hidden in password-protected and encrypted attachments and malicious URLs against a comprehensive cross-matrix of operating systems, applications and web browsers. FireEye Email Security can be centrally managed.

Organisations are migrating email services to the cloud. FireEye Email Security meets their security, data privacy, performance, and cost needs with a cloud-based email service for advanced threat protection. The FireEye data centre located in Frankfurt, Germany complies with SOC 2 Type II certification and General Data Protection Regulation (GDPR), enabling organisations to use state-of-the-art, cloud-based security to minimise breach opportunities—demonstrating its innovation cycle and commitment to solving the company’s customers’ biggest challenges.

FireEye Email Security automatically detects and stops emerging email-borne attacks from the first time they’re seen, providing instant insight into the attack and attacker, to simplify alert prioritisation and threat response.

It prepares organisations for future attacks based on intelligence derived from hundreds of thousands of hours of incident response engagement, a global network of sensors collecting real-time intelligence, and hundreds of analysts and researchers.

It ensures that intelligence feed updates are delivered in real-time with real evidence about newly detected attacks.

According to judges, its real time intelligence feeds provide updates to identify newly detected attacks making this a great enterprise solution.

Finalists 2018

- Highly Commended: Attivo Networks® ThreatDefend® Deception and Response Platform
- GuardiCore Centra Security Platform
- InsightIDR
- TrapX Security DeceptionGrid

Finalists 2018

- Highly Commended: Proofpoint Email Protection
- Agari Email Trust Platform
- Barracuda Essentials for Email Security
- Egress Switch
- FireEye Email Solution
- Glasswall FileTrust for Enterprise Email
Modern web browsers can now send reports when they observe events that may impact security. The company’s service, Report URI, allows websites to quickly and easily setup reporting by sending their reports to URI for processing instead of having to build their own infrastructure to handle and process the reports themselves. Any individual or company with a website can benefit from the insight that these reports can provide into real-time threats on their site.

Report URI caters for a variety of different security reports that browsers are capable of sending but the most sought-after reports are those about XSS (Cross-Site Scripting) attacks. Using a Content Security Policy, a website can both defend against these attacks and have the browser report back when it finds evidence that an attack has been attempted or has taken place. This allows a website operator to gain insight into threats their visitors are facing in real-time and take immediate action to respond and resolve the problem.

The ability for browsers to send these reports is relatively new and whilst some sites have experimented with reporting it’s only a tiny handful on the largest sites on the web that deploy this capability today because of how difficult it can be to do right. Its service allows any site operator, no matter how big or small, to deploy and enable reporting in a matter of minutes and start gaining immediate insight into threats that their visitors may be facing. This is a completely new source of information that sites can use to better protect themselves and their visitors.

According to judges, the product really fills an important niche in web security by enabling web server operators to make use of (the usually ignored) CSP reports. “While it is a very specialised solution and one can argue that the overall market capitalisation might be rather small, it is an important step in opening up a new type of intelligence products.”

Judges considered the product flexible and intelligent enough to protect all the company’s digital assets, whether on the network or in the cloud.
BEST ENTERPRISE SECURITY SOLUTION

WINNER
CrowdStrike Falcon

The CrowdStrike Falcon Platform is the only cloud delivered, next-gen endpoint protection solution that unifies next-gen AV, endpoint detection and response (EDR), managed hunting, IT Hygiene, threat intelligence, and vulnerability management. Due to its modularity, customers can choose whether to replace their AV for more effective protection or augment it with other modules.

Falcon is both lightweight and cloud-enabled, so customers can operationalise it at unprecedented speed and the lowest TCO. Falcon can be deployed within hours, it requires no hardware or additional software, no implementation services, no tuning or configuration and has virtually no impact on the endpoint. It is not uncommon when responding to a breach for the CrowdStrike Incident Response team to deploy and start using the Falcon sensor within hours across thousands of endpoints. This architecture, where the heavy lifting is performed in the cloud, allows customers to manage the solution and scale without worrying about additional cost, time and effort.

Its cloud-based architecture enables it to push out multiple updates and upgrades as needed with no disruption or interruptions to the user. Typically, CrowdStrike issues quarterly product updates with key new features, modules, and substantive additional capabilities. Additional updates might occur when required. The use of a machine learning model for malware prevention completely eliminates the need for daily signature updates. Last year CrowdStrike customers were instantly and automatically protected from WannaCry and NotPetya, the massive outbreaks that crippled hundreds of organisations worldwide.

Judges said that technically their whole service module is bang up to date with continuous improvement and excellent TCO/ROI.

BEST IDENTITY MANAGEMENT SOLUTION

WINNER
CyberArk Privileged Account Security Solution

The CyberArk Privileged Account Security Solution expands access control to any IT environment, from on-premises and hybrid cloud to DevOps, helping organisations prioritise risk management without sacrificing efficiency, productivity or innovation. Specifically, in DevOps, secrets - which consist of privileged accounts, SSH/API keys, passwords, certificates and more – can be misused or intentionally targeted and exploited by malicious attackers. The CyberArk solution is necessary to apply privileged account security concepts including identity, authentication, least privilege and auditing to these non-human network entities.

The CyberArk Privileged Account Security Solution is the only solution that was designed and built from the beginning for security and can easily extend to new cloud and DevOps use cases. It is based on the novel CyberArk Shared Technology Platform, which combines an isolated vault server, a unified policy engine and a discovery engine, providing scalability, reliability and unmatched security for privileged accounts. The CyberArk Digital Vault is an isolated and bastion hardened server offering segregation of duties, high availability, disaster recovery and unprecedented protection with multiple layers of security for market-leading protection.

All CyberArk products interact directly with the Vault using a proprietary protocol, allowing all products and components to benefit from the secure storage of keys, passwords, policy settings and audit logs.

The platform delivers enterprise-class security, scalability and high availability. Business benefits include superior vaulting technology with multiple security layers built-in for authentication, and encryption.

According to judges, the product comprehensively addresses issues of privileged access and is a robust, competent, well considered proposition.

Finalists 2018
- Highly Commended: Proofpoint Advanced Email Security
- BooleBox
- CrowdStrike Falcon
- IBM Resilient Incident Response Platform (IRP)
- Onapsis Security Platform

Finalists 2018
- Highly Commended: My1Login, IBM Identity Governance and Intelligence (IGI)
- AppGate SDP
- Balabit-Privileged Access Management Solution (PAM)
- CyberArk Privileged Account Security Solution
- One Identity, Identity Manager
BREACHES 
STOP HERE 
CAN'T STOP TODAY'S CYBER ATTACKS?
CROWDSTRIKE FALCON CAN.

FIND OUT MORE AT 
CROWDSTRIKE.COM/SEEDEMO
IBM Managed Security Services

IBM is an industry-leading Managed Security Service partner providing outstanding personalised protection from attacks, including in the cloud. IBM has differentiated itself by making significant investments in people, facilities, tools and cutting-edge cognitive technologies to provide a service built on industry-leading security intelligence and proven security methods delivered by experts located in eight global X-Force Command Centers (including two in Europe).

Leveraging X-Force Threat Research and Intelligence alongside new capabilities powered by Watson for Cyber Security, IBM has access to huge volumes of threat intelligence and real-world insights, that enable personalised protection from security threats. From 2017 all Threat Monitoring Clients using IBM QRadar also receive the cognitive QRadar Advisor app to be used by their MSS Threat Analysts, providing cognitive capabilities at no extra cost.

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

The service can be activated quickly, courtesy of 24x7 operations, with dedicated engineers and project managers, and adhering to a mature set of quality assured processes that guarantee systems are implemented and the service activated in line with industry best practices.

The MSS team can therefore operate a mature, tuned platform from day one and customers benefit from early reduction in exposure to threats and improvement in their security.

According to judges, impressive metrics and broad integrated functionality makes this a strong contender.

IBM MaaS360 with Watson UEM

Managing endpoints plus their users and data is a time-consuming task with conventional MDM and EMM solutions. Smart IT leaders are turning towards a cognitive UEM approach that consolidates the management of devices along with their data and apps.

IBM MaaS360 with Watson unified endpoint management (UEM) gives IT and security leaders one platform to manage and secure all their endpoints, including personal and corporate-owned devices, across iOS, macOS, Android and Windows platforms.

IBM MaaS360 with Watson offers one of the fastest and most cost-effective ways to meet new business challenges and support new users, devices, and apps. MaaS360 solutions run in the cloud and work seamlessly with your on-premises and cloud systems—reducing the effort needed to deploy, scale, maintain, and update. Updates are pushed down automatically from the cloud and require no maintenance or user intervention. Zero-day support is routinely available for all major supported operating systems.

MaaS360 goes well above the security offerings that come natively from device manufactures. Including mobile threat management for the remediation of malware and secure chat.

Judges said that this was a convincing product and solid solution with a broad range of features and some neat possibilities.
As the world becomes more connected, we make it more secure

You will find our identity and access management (IAM) solutions and data protection technologies at the heart of modern life. We are there when banks exchange funds, people cross borders or drivers step into connected cars.

Across time zones and continents, we protect businesses, governments and two billion people from data breaches and identity theft. By relying on us, our clients in 180 countries can offer trusted and secure digital services so that their customers and citizens can enjoy their digital lifestyles.

Put simply, through authentication and protection we offer the “security to be free”.

LEARN MORE
BEST NAC SOLUTION

WINNER
ForeScout CounterACT

ForeScout has pioneered an agentless approach to network security to address the explosive growth of mobile computing, cloud computing and the IoT. Outdated policies, such as ‘block everything that is not owned by the organisation’, stifle and disrupt business productivity. ForeScout CounterACT is a different type of network access control product that is built for today’s campus, data centre, cloud and operational technology environments.

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. In 2017, in over 70 countries, more than 2,500 customers with 850+ employees improved their network security and compliance with ForeScout.

Altogether, ForeScout is cost effective to run and lowers the expense of network management. It includes functionality within a single appliance, available physically or virtually. It also offers bi-directional integration to solve security and operational problems, allowing customers to make the most of existing security investments and resources while providing extensive information about the network, including vulnerable applications and processes.

CounterACT can provide a significant TCO improvement to customers’ operations 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.

Judges thought that it was a great differential to be agentless and have the ability to support such a broad range of devices.

Finalists 2018
- Bradford Networks
- ForeScout CounterACT
- Pulse Secure - Pulse Policy Secure

BEST NEWCOMER SECURITY COMPANY OF THE YEAR

WINNER
Panaseer

Panaseer’s core commercial offering includes the Panaseer Platform and corresponding professional and managed services tailored for the Enterprise market.

The product portfolio is strong and rapidly growing, serving a broad range of strategic and tactical cyber-security use cases. Currently the portfolio consists of core platform, deployed on-premise or cloud, with 40+ 3rd-party product integrations and workflow integrations. Strategic plans are in place to enable the creation of product integrations to external developer communities.

Panaseer is empowering Security teams with automated insight and remediation activities (efficiency gains). Using the platform increases the credibility of the Security team by giving them quick access to data to answer questions.

Customers have reported improved internal communications (eg. relationships between Security and Infrastructure teams because they can now provide access to ‘good news stories’ and have consistency of information being reported).

Judges thought that this is a credible newcomer to the cyber-security industry with refreshing product and service attitude that is being praised by CISO’s with genuine applause for its product as a developing “single go to” for a daily picture of security awareness of corporate infrastructure.

Finalists 2018
- Panaseer
- XM Cyber
Everyone Talks Visibility

We Actually Do It

You can’t secure what you can’t see™

See for yourself
www.ForeScout.com/demo
WINNER
ISACA / CISM

CISM is a management-level certification for information security professionals. Most security certifications measure the candidate’s understanding of security technologies and processes – CISM differentiates itself by also measuring the candidate’s understanding of how these processes support business goals.

Earned by more than 38,000 professionals since inception in 2002, CISM distinguishes certification-holders as possessing not only information security expertise, but also knowledge and experience in the development and management of an information security programme that protects organisational assets in alignment with organisational objectives. Five years of work experience is required, including a minimum of three years of information security management in several job practice analysis areas. ISACA’s global chapters network strongly supports the certification, offering exam review courses.

ISACA’s CISM certification allows professionals to meet employers’ demand for experienced information security managers who understand business concepts. Enterprises around the world are beginning to recognise that information security must be strongly represented at the upper levels of an organisation, making the CISM credential increasingly critical for individuals who develop, build and manage enterprise information security programmes.

Strong security programmes must be aligned to overarching enterprise goals to deliver the desired results.

According to judges, the certification’s real value-add is how CISM teaches candidates the importance of how security processes support and enable business goals. This is a critical component of a security professional in today’s industry where security has to be sold and perceived by boards as a business-enabling capability and not a restraint.

BEST RISK MANAGEMENT/REGULATORY COMPLIANCE SOLUTION

WINNER
Skybox Security Suite

Skybox Security has more than 700 customers in over 50 countries and nearly every industry. 40 percent of Skybox customers are ranked on the Global 2000 list of the world’s largest enterprises.

Skybox Professional Services offers extensive end–user and administrator training, deployment customisation, system integration, ongoing mentoring and more. Skybox Professional Services has also started offering a health check service for in-depth consultation to evaluate deployments and recommend fixes, optimisation or new features.

Skybox has already taken steps to extend the security management capabilities to virtual and cloud networks, as well as operational technology found in critical infrastructure organisations. Further analysis, automation and orchestration capabilities will be added in 2018. Expanded firewall change provisioning, tools for incident response and SOCs are also on the company’s roadmap for 2018. Skybox has also begun transitioning to a completely web–based UI to improve user experience.

In addition, Skybox has created a customer advisory board and cyber-management advisory to engage customers and identify challenges that in turn will influence Skybox’s technical strategy.

Skybox provides literal attack surface visibility through an interactive visualisation layer based on its network and risk modelling capabilities. Simulations, attack vector analyses and threat–centric vulnerability analyses provide contextual intelligence specific to the enterprise. Integration with 120+ networking and security technologies extracts more value.

Judges said that it is great to see that the company has extended its service to virtual and cloud networks, and have focused on operational technology within CNI, which is an oft-ignored sector and critically important.

Finalists 2018

• ISACA CISM
• Highly Commended: ISACA CRISC
• Cybersecurity and Criminology Centre: Doctorate Training Programme, University of West London
• ISACA CISA
• Secure Code Warrior
• Wombat Security Technologies’ Product Portfolio

Finalists 2018

• Highly Commended: OneTrust Privacy Management Software
• AlgoSec Security Management Solution
• Skybox Security Suite
• SureCloud Platform - Risk Management and EU GDPR Applications
• Varonis Data Security Platform
BEST THREAT INTELLIGENCE TECHNOLOGY

WINNER
Recorded Future

Recorded Future aims to deliver the only complete threat intelligence solution powered by patented machine learning to lower risk. The company empowers organisations to reveal unknown threats before they impact business and enable teams to respond to alerts ten times faster. To supercharge the efforts of security teams, the company’s technology automatically collects and analyses intelligence from technical, open, and dark web sources and aggregates customer-proprietary data.

Recorded Future delivers more context than threat feeds; it updates in real time so intelligence stays relevant, and it centralises information ready for human analysis, collaboration, and instant integration with security technologies. 91 percent of the Fortune 100 use Recorded Future.

Its customers gain a combination of real-time and relevant context, all in a single view, without the ability to dig deeper for more information. Recorded Future has a broad view of the threat landscape, and is believed to have more data in more languages than any other provider, including deeper dark web coverage and analysis.

This combination of machine learning with finished intel from its team of researchers delivers intelligence at incredible speed and scale. Inside Recorded Future organisations can also fuse the company’s intelligence with any other sources of threat data including their own analysis, making its product both a provider and a platform for working with threat intelligence.

The Recorded Future solution is modular, allowing organisations to invest in what they need today with the option to expand functionality overtime all based on the foundational Recorded Future Threat Intelligence Machine. Organisations can add users and integrations as well as take advantage of access to analysts on-demand.

Judges said that this was a great product offering in all key areas for gaining and using the intelligence.

BEST USE OF MACHINE LEARNING/AI

WINNER
ImmuniWeb

For large companies, ImmuniWeb reduces application security testing costs and centralises application security testing into one single platform. The platform provides flexible access control and role management for internal security teams, application developers and even for external vendors if required. ImmuniWeb has several Technology Alliance Partnerships with the global WAF leaders, such as F5 and Imperva, to provide reliable (ie false-positive free) instant virtual patching in just one click.

Finally, cyber-security teams of large organisations can devote their precious time to various complicated problems, while the solution take care of their web and mobile application security. For SMEs, ImmuniWeb provides flexibility and 24/7 expert support from the company’s SOC. Any questions about vulnerability remediation, exploitation or related risks are usually answered in less than 30 minutes, seven days a week. ImmuniWeb delivers all-inclusive application security testing and remediation for a very competitive price, bringing a peace of mind to SMEs who don’t want to spend too much time on security of their websites and mobile apps.

ImmuniWeb substantially reduces all spending on AST human power: companies don’t need to spend any more on manual testing, false-positive triage and puzzle over vulnerability analysis and remediation.

ImmuniWeb eliminates licence costs of many automated solutions by providing reliable and top-quality application security testing service from A to Z.

Indirect cost saving comes from availability of client’s workforce for other internal challenges that can be timely mitigated without increasing risks or adding costs.

According to judges, ImmuniWeb Platform leverages numerous ML/AI algorithms for intelligent automation of costly tasks that previously required human labour.

Finalists 2018
• Highly Commended: IBM X-Force Exchange, EclecticIQ Platform
• AlienVault Open Threat Exchange (OTX)
• CrowdStrike Falcon Intelligence
• DFLabs IncMan
• Recorded Future
• RiskIQ PassiveTotal
BEST SIEM SOLUTION

WINNER
Exabeam Security Intelligence Platform

Recent data breaches suggest that SIEM as a security management solution, is broken. Attacks using stolen or misused passwords are on the rise, with companies struggling to detect or respond to them effectively. Exabeam’s Security Intelligence Platform (SIP) decreases the risk of cyber threats for any organisation. It incorporates a completely new approach to data protection, relying on modern analytics, automation, and human expertise.

Traditional SIEM products are no longer able to detect credential-based attacks, whether from a hacker using stolen passwords, or from a malicious employee using their own access rights. Traditional SIEM products also limit data collection by charging by the byte. Nearly every company that suffered from a public breach in recent years had a SIEM system in place at the time. Modern security organisations deserve better. SIP is designed to be the first security management platform to fully deliver on the initial “promise of SIEM”: complete visibility into modern threats and automated, intelligent response.

Exabeam’s data collection leverages the well-proven open source ElasticSearch platform for unlimited scalability, but it does not use a volume based pricing model, instead opting for a flat licensing model. This combination enables customers to capture, search and analyse ALL security data generated and will continue to do so as data volumes grow.

Threat detection comes from one of the most widely-deployed user behaviour analytics technologies available today (Exabeam UEBA). This enables analysts to track lateral movement and detect the attacks behind almost every data breach.

Exabeam includes automated incident response.

Judges said the product addresses the three weaknesses of traditional SIEM; data collection, threat detection and incident response.

BEST SME SECURITY SOLUTION

WINNER
Proofpoint Essentials

Proofpoint Essentials offers a follow-the-sun support with very high-level consistency and high levels of customer service satisfaction scores. Globally, customers have access to 24x7x365 support within the Proofpoint Essentials subscription with phone, email and live chat communication options available.

The Proofpoint Essentials support team continually adds to the knowledge base library of technical videos to help onboard new customers and provide existing customers with references to numerous product features.

Proofpoint Essentials is a cloud-based, user-friendly service with a low total cost of ownership. Costs of infrastructure management and updates are included in the annual subscription. As Proofpoint Essentials is cloud-based, customers can be up and running in minutes. Administrators can access all elements of email security, social media security and archive through a single portal reducing management costs for IT. The intuitive interface makes it easy for the administrator to manage policies and users.

The end-user experience is specifically designed to limit the need for IT interaction. End-users can access their email quarantines, email continuity or archive through easy-to-use web-based tools and integrations.

Small businesses are targeted by the same threats as large enterprises and Proofpoint Essentials protects SMEs from these threats including ransomware, malicious attachments and URLs, email fraud, which includes business email compromise attacks, and credential phishing. Proofpoint Essentials also helps organisations secure their social media channels and protect their customers from any malicious URLs posted by users.

Judges felt that Proofpoint has done well in extending its enterprise-level capabilities into a service that is affordable and meets the needs of the SME market.
BEST SECURITY COMPANY

WINNER
Rapid7

Rapid7 has seen strong and steady growth of its customer base across all products and services - from 1,750 customers at the end of 2011, to more than 6,500 in 120 countries in 2017. In Q2 2017, total revenue had increased by 27 per cent since the same time the previous year. Additionally, Rapid7 experienced 17 per cent growth in its customer base since Q2 of 2016.

Rapid7 is trusted by IT and security professionals around the world to manage risk, simplify modern IT complexity, and drive innovation. Rapid7 analytics transform today’s vast amounts of security and IT data into the answers needed to securely develop and operate sophisticated IT networks and applications. Rapid7 strives to foster customer engagement through ‘Lunch and Learn’ and ‘User Group’ events, as well as a ‘Voice’ programme, an online community where customers can engage with one another as well as Rapid7 representatives.

Grounded in security research, data analytics, and an excellent understanding of the attacker mind-set, Rapid7’s products and solutions enable organisations to strategically manage their cyber-security exposure. Once implemented, organisations are able to prevent and contain live threats, gain visibility into vulnerabilities, respond to breaches, and correct the underlying causes of attacks.

With the evolution of the Rapid7 Insight platform—believed to be the first and only cloud-based platform to combine vulnerability management, user behaviour analytics-powered SIEM, application security, and IT log analytics—organisations are more equipped than ever to collect data, transform it into prioritised and actionable insight, and get it to the people who can act on it. Acquisition of Komand cuts ecosystem complexity.

The judges said that the company had an extensive product and services portfolio with good customer service capability, research capability and community involvement.

BEST SECURITY TEAM SPONSORED BY CROWDSTRIKE

WINNER
Royal Bank of Scotland

The security team has developed and managed itself to be invaluable within the corporate environment – particularly seeing as cyber-crime is such an important concern for financial organisations.

The team has worked to position cyber-security as a critical business issue by actively engaging with leaders and colleagues. This is evident in the fact that information security and cyber-security are formal components of RBS’s Risk Management Framework. This Framework was restructured 18 months ago to integrate IT Security within general Security; as well as this, cyber-security is embedded in the business through the bank’s “Three Lines of Defence” model which includes: Management & Supervision; Oversight & Control; and Internal Audit. This framework and the defence model are applied to every part of the business, so all staff understand their individual and collective responsibilities.

Due to this internal commitment, and monetary investment in cyber, RBS has seen a huge decrease in fraud levels.

The team works with brand and marketing to win hearts and minds by promoting the importance of cyber-security to both colleagues and customers – the same messages that are in the bank’s TV adverts are shared with staff through internal initiatives, such as bank-wide brainstorm sessions and cyber-security training.

Furthermore, cyber-security is part of employee performance evaluation. All permanent RBS employees and temporary contractors must complete a targeted Group Policy Learning (GPL) programme. Failure to adhere to cyber-security policies is treated very seriously and may even lead to disciplinary action. Also the team comprises subject matter experts who share their knowledge.

According to the judges, the team has a huge focus on user awareness throughout response showing good business focus for the security programme.

Finalists 2018

• Highly Commended: Symantec
• Duo Security
• FireEye
• Proofpoint
• Rapid7
• Sophos

Finalists 2018

• Highly Commended: Knights of Security (Manchester Airport)
• Royal Bank of Scotland
• Stiftung Wagenhof Foundation
Vulnerability management hasn’t kept pace with the adoption of cloud, containers, web applications and the convergence of IT and OT. Headlines around Equifax and WannaCry underscore the importance of understanding and protecting the modern attack surface. To solve this challenge requires comprehensive visibility into any asset on any computing platform. Using the Nessus technology deployed by 1.6 million users, Tenable.io combines active and agent-based scanning, continuous passive monitoring, and container image scanning to eliminate blind spots across IT, cloud, and IoT environments. It provides continuous visibility into all assets (managed and unmanaged) on an organisation’s networks, making it possible to see and secure the complete attack surface. This combination of data collection technologies, open API and SDK, and tailored prioritisation enables security teams to see more (like containers, IoT, and industrial control systems), and do more (by understanding and acting on what matters most).

Tenable.io says it is the first vulnerability management platform to provide visibility across the full range of assets, including IT, OT and IoT. It is also believed to be the first and only VM solution to provide continuous visibility into managed and unmanaged assets, using Tenable’s patented Nessus Network Monitor technology.

Tenable.io also has integrated container security capabilities in a complete vulnerability management solution.

According to the judges, Tenable has built upon the Nessus technology to deliver a slick, open and integrated product that is very capable of managing today’s diverse enterprise architectures. The elastic licensing model, coupled with its ability to manage assets as opposed to an identity based purely on IP address are also worthy of mention.
Carbon Black.

Serious Protection Starts with the Predictive Security Cloud

Find out more at www.CarbonBlack.com
The growing demand for cyber-security professionals has led both government and industry to introduce initiatives to increase the range and variety of cyber-security relevant courses, supplemented by competitions that also draw in mature students and non-STEM candidates.

Now there are GCHQ accredited cyber-related Masters, competitions for schools, universities, and open access. There are brilliant individual students conducting both theoretical and practical research, up to and including the launch of new products and services, and there are teams of students banding together to take on the challenge of simulations.

There are girls-only courses and competitions, and events to bring in other under-represented groups, including those targeting neural-diversity to ensure all talents that might contribute are represented in the industry.

This year’s winners, Team CDT - Georgia Crossland, Amy Ertan, Lydia Garms and Angela Heeler, students at Royal Holloway, University of London, are also winners of the Atlantic Council UK Cyber 9/12 Policy Competition 2018.

This competition entailed demonstrating, within a competitive environment, not just ability to identify, comprehend and manage appropriate response to a simulated cyber-attack, but also to be able to effectively communicate what was happening to non-specialist government decision makers - the Prime-Minister’s advisors. Thus, they needed to show both technical and operational skills as well as strategic risk analysis, turning data into actionable intelligence at both the operational and strategic level. Truly a test of the skills we need in our CISOs of the future.

Andrew Rose is the organisation’s CISO and head of Cyber Security. Under his tenure, NATS has taken the path to ISO27001 certification. NATS is the third organisation that Rose has led to this renowned certification.

This is not the first time NATS or Rose has been recognised by the industry. The NATS Security and Cyber Security team won Best Security Team at the 2014 SC Awards Europe.

In 2017, Rose joined the Professional Advisory Board of CyBOK, contributing to the development of a comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector.

According to judges, Andrew is a true expert in cyber-security, combining technical expertise with theoretical and analytic understanding of the issues faced to provide strong leadership of an excellent team at NATS, using his communication skills to promote the importance of cyber-security issues both internally as well as within the wider critical national infrastructure sector.

Winner 2018
Andrew Rose, CISO and head of cyber security, NATS
We confidently face security threats.
So you can confidently face your customers.

IBM Security tackles the world’s most challenging security problems. We continually look for new and better ways to protect the faces behind the data – your customers. Our strategy reflects our belief that today’s defenses will not suffice tomorrow. It challenges us to approach our work, support our clients and lead the industry with forward-thinking solutions that leverage cloud, AI, orchestration, and collaboration.

Face your customers with confidence.
Let IBM Security be your trusted advisor.