JD Wetherspoon attack took 15 mins says hacker 'Ropertus'

29 locations affected in Elephant Bar POS breach

Anonymous declares 'trolling day' on ISIS

November 2015 Issue

Editorial

Pushing past shock and yawn

Threat of the month

Threat of the Month, November 2015

Subscribe

Archive

Staff Report

December 10, 2015

2016 SC Awards U.S. Finalists

Share this article:

GROUP 1

2016 SC Awards U.S. Finalists

READER TRUST AWARDS

Best Advanced Persistent Threat (APT) Protection

An advanced persistent threat (APT) product and/or service provides real-time detection of and protection against intruders gaining access to an enterprise environment to stealthily extract high-value information assets from targeted organizations in manufacturing, financial, national defense and other industries.

Check Point Software Technologies for SandBlast

eSentire for Active Threat Protection

FireEye for FireEye Threat Prevention Platform and Services

Invincea for Invincea Advanced Endpoint Protection

RSA, The Security Division of EMC for RSA Security Analytics

Best Mobile Security Solution

More and more employees are using smaller and smaller devices with loads of applications to access corporate data. Some examples include iPhones, iPads, Android devices, BlackBerries and more. Products in this category deal with not only a collapsing perimeter, but also consumer-owned and -controlled devices being used to get at corporate resources. At a minimum, these devices likely will require strong endpoint security, point-to-point encryption and more. This is a broad category. If your product is used to secure this type of small device/handheld, it may fit. Security can be for data at rest in the device itself, secure access to data in the enterprise, and encryption for data in motion between the enterprise and the device. It also includes anything from hard disk encryption solutions and tools that track lost mobile devices to USB/thumb drive security solutions.

AirWatch for AirWatch by VMware Enterprise Mobility Management

INSIDE Secure for Matrix SSE

Proofpoint for Proofpoint Targeted Attacked Protection (TAP) Mobile Defense

Skycure for Skycure Mobile Threat Defense

Wandera for Secure Mobile Gateway

Best Vulnerability Management Solution
These products perform network/device vulnerability assessment and/or penetration testing. They may use active or passive testing, and are either hardware- or software-based solutions that report vulnerabilities using some standard format/reference.

BeyondTrust for Retina CS Enterprise Vulnerability Management

Core Security for Core Insight

NopSec for Unified VRM

Rapid7 for Nexpose

Tenable Network Security for Nessus Cloud

EXCELLENCE AWARDS

Best SME Security Solution
This includes tools and services from all product sectors specifically designed to meet the requirements of small- to midsized businesses. The winning solution will have been a leading solution during the last two years, having helped to strengthen the IT security industry's continued evolution.

Barracuda for Barracuda NG Firewall

Network Box USA for Network Box USA SME Security Solution

Netwrix for Netwrix Auditor

TraceSecurity for TraceCSO

Untangle for NG Firewall

GROUP 2

READER TRUST AWARDS

Best Cloud Computing Security Solution
These technologies are deployed to protect data and/or applications in a cloud environment. They may also protect the cloud computing infrastructure itself. Cloud computing security concerns are numerous for both providers and their customers – and include security and privacy worries, compliance issues and legal/contractual problems. Solutions or services in this category can provide for the protection of data or applications in the cloud, protection for traffic flowing between companies and their cloud service providers, policy management and encryption capabilities, privileged user access and controls or more.

Dell for Dell Cloud Access Manager 8.1

Illumio for Illumio Adaptive Security Platform

Netskope for Netskope Active Platform

Skyhigh Networks for Skyhigh Cloud Security manager

Zscaler for Zscaler Next Generation Firewall

Best Fraud Prevention Solution
Given the reliance on the internet by consumers from all walks of life to conduct any number of retail, banking or other transactions, fraud prevention solutions have become critical. Tools nominated in this category strive to minimize online privacy and security problems that could lead to fraud and, therefore, impact both the company and the customer. Still an evolving area of information security, there are a slew of solutions and services available that could qualify for consideration in this category – from authentication and enhanced encryption solutions to secure web communication or malware-detection offerings.

Easy Solutions for Total Fraud Protection

Equifax for FraudIQ Manager

RiskIQ for RiskIQ

Sift Science for Sift Science Fraud Prevention

Splunk for Splunk Enterprise

Best Multifactor Solution

Products here provide enhanced security to end-users or devices by offering credentials for access to an authenticator or authentication server. Software and hardware that specializes in the biometric authentication of users is also included here. These solutions may use a tangible device (something you have) for authentication and knowledge (something you know) for authentication. For biometrics, the solution provides identification and authentication using any of the following methods: finger/thumb print/retinal scan/voice recognition/hand/palm geometry/facial recognition.

MicroStrategy Usher for Usher Mobile Identity Platform

Nok Nok Labs for Nok Nok Labs S3 Suite

RSA, The Security Division of EMC for RSA SecurID

SecureAuth for SecureAuth IdP

Yubico for YubiKey NEO

Best Web Application Solution

Application firewalls inspect the body of packets and restrict access to legitimate application traffic while blocking access to other parts of the operating system. They typically use deep-packet inspection, provide logging and reporting, block real-time traffic, provide alerting capabilities and auto-update features, perform web caching, provide content filtering, offer web-based access to reporting and/or logging, protect traffic from reaching the underlying operating system, and filter application traffic to only legitimate requests.

Alert Logic for Alert Logic Web Security Manager

Barracuda for Barracuda Web Application Firewall

F5 Networks for F5 BIG-IP Application Security Manager (ASM) and F5 Silverline Web Application Firewall (WAF) service

iboss Cybersecurity for iboss Secure Web Gateway

Palo Alto Networks for PA-7080

EXCELLENCE AWARDS

Best Enterprise Security Solution

This includes tools and services from all product sectors specifically designed to meet the requirements of large enterprises. The winning solution will have been a leading solution during the last two years, having helped to strengthen the IT security industry's continued evolution.

Cisco for Cisco's AMP Threat Grid

Cyphort for Cyphort Advanced Threat Defense Platform 3.3

Digital Shadows for Digital Shadows SearchLight

Palo Alto Networks for Palo Alto Networks Next-Generation Security Platform

Skyhigh Networks for Skyhigh Cloud Security Manager

GROUP 3

Best Computer Forensic Solution

Products in this category fall into two sub-categories: network and media. The network tools must be exclusively intended for forensic analysis of network events/data. If the product is a SIEM with forensic capabilities, it should be placed in the SIEM category. Media tools cover just about all other non-network forensic tools, including those tools that collect data from media over the network and live forensic tools. This also includes specialized forensic tools that are not intended to analyze network data.

AccessData for Forensic Toolkit (FTK)

Blue Coat Systems, Inc. for Blue Coat Security Analytics Platform

FireEye for Network Forensics Platform and Investigation Analysis Platform

Guidance Software for EnCase

LogRhythm for Network Monitor

Best Identity Management Solution

Products in this category address the identity management lifecycle in an enterprise environment, including password management, user provisioning and enterprise-access management.

CyberArk for CyberArk Privileged Account Security Solution

Dell for Dell One Identity Manager 7.0

Identity Automation for RapidIdentity

Identiv for Identiv Connected Physical Access Manager (ICPAM)

Ping Identity for Identity Defined Security platform

Best NAC Solution

network resources from threats that are brought in by employees, vendors, contractors and guests involves a numbers of solutions and policies. From anti-virus and firewalls to IDS/IPS solutions, the products in this category run the gamut. However, to control access to network resources at the endpoint, the tools companies often rely on are network access control (NAC) products. These solutions can be used to validate the existence of certain security measures and validate that they are properly configured and up to date. They also can validate the existence of current OS patches and can be used to manage the complexity associated with overseeing permissions and authorizations for various groups of users. Most will integrate with a common directory structure, some will provide local authentication capabilities, while others will match something on the endpoint − such as an agent or MAC address − to the authentication before allowing access to the protected network resources.

Cisco for Cisco's Identity Services Engine (ISE)

Cryptzone for AppGate

ForeScout Technologies for ForeScout CounterACT

Pulse Secure for Pulse Policy Secure

Trustwave for Trustwave Network Access Control

Best Behavior Analytics/Enterprise Threat Detection

A still somewhat-emerging category, these products focus on detecting insider threats, targeted attacks and other fraudulent activities by examining human behaviors, sussing out patterns that are then analyzed through the application of algorithms and statistical analysis to detect anomalies that may indicate threats of loss or compromise to organizations' critical data. Offerings in this space are also referred to as so-called "user behavior analytics" products by analyst company Gartner.

Gurucul for Gurucul GRA

Masergy Communications, Inc. for Unified Enterprise Security (UES)

Rapid7 for UserInsight

Splunk for Splunk UBA

Vectra Networks for Vectra Automated Threat Management solution

EXCELLENCE AWARDS

Best Regulatory Compliance Solution

Nominated solutions should help organizations comply with specific regulatory requirements demanded of companies in the health care, retail, educational, financial services and government markets. Solutions should help customers meet mandates noted in such legislation as HIPAA, SOX, GLBA, FISMA, or in guidelines noted by the likes of the FFIEC or the PCI Security Standards Council. Nominees must be prepared to offer references of customers who are engaged in, or have already completed, real, fully fledged deployments, and should be ready to address specific questions posed to them during the judging process.

Agiliance for RiskVision 7.5

Netwrix for Netwrix Auditor

RSA, The Security Division of EMC for RSA Archer GRC

Tenable Network Security for SecurityCenter

Trustwave for Trustwave TrustKeeper

GROUP 4

Best Data Leakage Prevention (DLP) Solution

Products in this category include those that help organizations safeguard their intellectual property and customers' critical data persistently – inside and outside the company. Network-based and endpoint data leakage prevention products will be considered. Products should prevent data from unauthorized exit from the network, or protect data on the endpoint – whether the endpoint is connected to a network or not. Products typically are policy-driven and should include scanning of all data, regardless of protocol or application leaving the network, and/or keep track of peripherals, such as removable storage and attached to the endpoint – reporting that inventory to a central location or administrator. All entrants should have the capability of being managed by a centralized administrator. Those products considered part of this category include: network DLP products, which are typically gateways; those products protecting only endpoints; and hybrid products that operate at both the gateway to the network and at the endpoint. Specifically for endpoint DLP, traffic should be monitored and encryption should be available.

AirWatch for AirWatch by VMware Enterprise Mobility Management

Clearswift for Adaptive Redaction

Dell for Dell Data Protection | Encryption

Digital Guardian for The Digital Guardian (DG) Data Protection Platform

Secure Islands for IQProtector

Best Risk/Policy Management Solution

These products measure, analyze and report risk, as well as enforce and update configuration policies within the enterprise, including but not limited to network, encryption, software and hardware devices. Contenders' products should offer a reporting format that covers the frameworks of multiple regulatory requirements, such as Sarbanes-Oxley, Gramm-Leach-Bliley and other acts and industry regulations. As well, this feature should be network-centric, providing reporting to a central administrator and allowing for companies to centrally manage the product.

So, overall, entrants' products should be enterprise-centric; collect data across the network, including threats and vulnerabilities; report associated risk, endpoint configuration, enforcement, auditing and reporting; provide remediation options (but are not exclusively patch management systems); and, finally, offer centralized reports based on regulatory requirements and local policies.

Bay Dynamics for Risk Fabric

SolarWinds for SolarWinds Network Configuration Manager

TraceSecurity for TraceCSO

Trustwave for Trustwave TrustKeeper Compliance Manager

Venafi for Trust Protection Platform

EXCELLENCE AWARDS

Best Customer Service

Support as well as service of products and assistance sold are critical components of any contract. For many organizations that seek out help from information security vendors and service providers, the aid they receive from customer service representatives is crucial to the deployment, ongoing maintenance and successful running of the technologies they've bought and to which they have entrusted their businesses and sensitive data. For this new category, we're looking for vendor and service providers that offer stellar support and service – the staff that fulfilled its contracts and maybe even goes a little beyond them to ensure that organizations and their businesses are safe and sound against the many threats launched by today's savvy cybercriminals.

Barracuda

Biscom

CipherCloud

Protegrity

Rapid7

PROFESSIONAL CATEGORIES

Best Professional Certification Program

Programs are defined as professional industry groups offering certifications to IT security professionals wishing to receive educational experience and credentials. Entrants can include organizations in the industry granting certifications for the training and knowledge they provide.

International Association of Privacy Professionals for Certified Information Privacy Professional

ISACA for CISA

ISACA for CISM

ISACA for CSXP

(ISC)² for Certified Information Systems Security Professional (CISSP)

Best IT Security-related Training Program

This category is targeting companies and organizations that provide end-user awareness training programs for organizations looking to ensure that its employees are knowledgeable and supportive of the IT security and risk management plans. It also is considering those training companies or organizations that provide programs for end-user organizations' IT security professionals to help them better address components of their IT security and risk management plans, such as secure coding, vulnerability management, incident response/computer forensics, business continuity/disaster recovery, etc.

Cybrary

Global Learning Systems

Phishme

Security Mentor

Wombat Security Technologies

GROUP 5

Best Database Security Solution

Protecting its critical information is the number one priority for many organizations. An integral component of this is to secure corporate databases. Entries here should include solutions that help customers safeguard mission-critical database environments. Features of these offerings can run the gamut – from encryption to access management to logging and monitoring. Be sure to explain the specific ways the solution protects these corporate crown jewels and the features present to ensure exposures are mitigated.

Netwrix for Netwrix Auditor

PHEMI Systems for PHEMI Central Big Data Warehouse

Protegrity for Protegrity Database Protector

Trustwave for Trustwave DbProtect

Vormetric for Vormetric Data Security Platform

Best Managed Security Service

These offerings provide a turnkey approach to an organization's primary technical security needs. These offerings can either be a co-located device at the client organization facility, or can be a completely outsourced solution where the application to be protected would reside at the vendor's data center.

Alert Logic for Alert Logic Cloud Defender

Digital Guardian for The Digital Guardian Managed Security Program

Netsurion for Netsurion remotely-managed network and data security services

Radware for Attack Mitigation Service

Radware for Hybrid Cloud WAF Service

Best SIEM Solution

Security information and event management (SIEM) tools are used to collect, aggregate and correlate log data for unified analysis and reporting. Typically, these tools can take logs from a large number of sources, normalize them and build a database that allows detailed reporting and analysis. While forensic analysis of network events may be a feature of a SIEM, it is not the only feature, nor is it the primary focus of the tool.

AlienVault for AlienVault Unified Security Management (USM) platform

Hewlett-Packard for HP ArcSight ESM (Enterprise Security Manager)

LogRhythm for Security Intelligence Platform

NTT Com Security US for Advanced Security Operations Center (ASOC)

Splunk for Splunk Enterprise Security 4.0

EXCELLENCE AWARDS

Best Security Company

Nominees should be the tried-and-true, longer-standing companies which have been offering products and services to customers for at least three years. Nominations can come from all sectors. Areas that will be accounted for in the judging process include: product line strength, customer base, customer service/support, research and development, company growth and solvency, innovation and more.

Cisco

CrowdStrike

FireEye

Palo Alto Networks

Zscaler

Rookie Security Company of the Year

Nominated companies should be new to the IT security field – offering an initial, strong, flagship product that is within two years of its initial release. Nominees can come from any IT security product/service sector and will be continuing efforts in further product development, customer growth and overall fiscal and employee growth. Please note in your submission the launch date of your initial flagship offering. If this initial offering or any of your other products have been on the market for longer than two years, please do not submit a nomination in this category.

Cybereason

HackerOne

iSIGHT Partners

Onapsis

ProtectWise

GROUP 6

Best Email Security Solution

Email security addresses the ability to exchange email messages with assurance, as well as the ability to filter email messages based on content, source or other criteria. Solutions should ensure

the privacy of sensitive messages, limit the repercussions of email forgery, and manage other aspects of safeguarding email within the organization. These products are enterprise-centric and should have, but are not required to have, some form of centralized management. They may include spam filters, junk mail filters, malware filters, unauthorized content (sometimes called "extrusion protection" or "data leakage protection"), phishing and other types of undesirable content. However, these are not simply anti-spam filters. These email security products should be evaluated on their effectiveness, manageability, non-intrusiveness, ease of use and other factors that impact the implementation of this type of product in the enterprise environment. They typically provide features such as email encryption, digital signatures, automatic shredding of messages and attachments, and more.

Cisco for Cisco's Email Security Appliance (ESA)

FireEye for FireEye EX series

HP Data Security for HP SecureMail

Proofpoint for Proofpoint Enterprise Protection Solution

Raytheon|Websense for Raytheon|Websense TRITON® AP-EMAIL

Best UTM Security Solution

Given the continuous convergence of the market, we've decided to retire some categories this year and integrate a number of individual categories from previous years into this unified threat management (UTM) category. The former categories – Best Enterprise Firewall, Best Intrusion Detection System/Intrusion Prevention System Product, Best IPsec/SSL VPN, Best Anti-Malware Gateway and Best Web Content Management – are now integrated here. As formerly, contenders in the UTM security category should take an "in-depth" defense approach. Entrants should have an integrated, multifunction endpoint/UTM offering – not a single-function product. These products typically aggregate a wide variety of threat data into a single unified tool. Many organizations define those threat categories as anti-malware, content management, IDS/IPS and spam filtering, along with firewall/VPN. Entrants should meet this minimum functionality and can include anti-malware gateway, anti-spam gateway and anti-phishing gateway, as well as provide web content filtering for laptops, desktops and, optionally, servers that blocks or filters objectionable websites and content.

Barracuda for Barracuda NG Firewall

EdgeWave for EPIC Next Generation Firewall

Network Box USA for Network Box USA UTM Security Solution

RedShift Networks, Inc. for UCTM Appliances

Sophos for Sophos SG Series UTM

EXCELLENCE AWARDS

Best Emerging Technology

What cutting-edge technologies with some innovative capabilities are bursting onto the scene to address the newest information security needs facing organizations? This new category welcomes both new vendors and old pros looking to provide products and services that look to help shape the future by addressing fast-evolving threats through the creation of these types of offerings. Solutions should have just hit the market in the last six to 12 months, and entries should have some customers available who can act as references. The company should also have an office in North America and provide ready support and service to customers in this country.

Bay Dynamic for Risk Fabric

CipherCloud for CipherCloud Platform

SentinelOne for SentinelOne Endpoint Protection Platform

Soltra for Soltra Edge

Twistlock for Container Security

PROFESSIONAL CATEGORIES

Best Security Team
Contenders should only include teams from end-user companies that have executed and are managing exceptional and strong security programs, which they have built from virtually non-existent ones. The team should have successfully established and implemented an integral and/or innovative/cutting-edge component of their security program, and should have spearheaded various areas of support for its success, such as strong end-user awareness training, good configuration management, and more.

Please note: Professionals who work for an IT security vendor, IT reseller or IT consultancies are not eligible for this category.

Goodwill

Voya Financial

Zuora

CSO of the Year
Contenders should include those who work for end-user companies only. No vendor CSOs will be considered. Nominees [illegible]ream of the crop, having spearheaded a viable IT security program, gained the s[illegible]their company's executive leaders, as well as their colleagues, and helped – through their indefatigable efforts – to propel the CISO/CSO position to a footing of influence within their organization and the corporate world as a whole. Specific projects and undertakings, as well as over-arching security programs to propel these various goals, should be noted. Nominees should be prepared to answer further questions during the judging process, offer at least two references, and be open to holding confidential interviews with members of the SC Magazine editorial team, if warranted.

Please note: Professionals who work for an IT security vendor, IT reseller or IT consultancies are not eligible for this category.

Bruce Wignall, CISO, Tel[illegible]mance

Michael Echols, CISO, M[illegible]a County

Michael Roling, CISO, State of Missouri, Office of Administration

Pritesh Parekh, VP, Chief Security Officer, Zuora