CSO OF THE YEAR

Building programs and guarding against future threats are all in a day’s work for Experian’s Stephen Scharf  P18

Canada’s cloud opportunity
Could Canada be a haven for companies nervous about online storage in the United States?  PC1

Hacktivism endures
Despite making arrests, authorities seem little closer to stopping the new face of social protest  P24

FEATURES:

REVIEWED IN GROUP TESTS

- **Adtran P34**
  - Full-featured UTM appliance with many deployment options

- **Astaro P35**
  - Solid gateway protection at a reasonable price

- **Fortinet P38**
  - Affordable, purpose-built UTM tool for smaller networks
ADVANCED TARGETED ATTACKS HAVE PENETRATED 95% OF ALL NETWORKS. THINK YOU’RE IN THE 5%?

You may think your existing security defenses prevent advanced targeted attacks from entering your network and stealing your data. They don’t. Advanced attacks easily evade traditional and next generation firewalls, IPS, AV and gateways. Your best defense is FireEye. Trusted by the Fortune 500, FireEye is the leader in helping enterprises combat advanced malware and targeted APT attacks.

Put a stop to advanced attacks with advanced security. Visit us today at www.FireEye.com/StopAPTs and let us help you close the hole in your network.

© 2012 FireEye. All rights reserved.
Editorial

Stern oversight in the United States

At the same time that the FBI and the U.S. Department of Homeland Security announced their plans to monitor social media sites in real time, the European Court of Justice (EU Court) was making a completely different call about the info people share on these networks.

U.S. agencies argue that monitoring social media will arm them with “situational awareness” to thwart potential attacks against the country and its critical infrastructure. The FBI, however, touted in a recent Computer World article its planned legal review of these activities to ensure it doesn’t compromise privacy or civil rights.

Across the pond, meanwhile, publishers and copyright holders were attempting to force social media outlets to use filters to help stop illegal file sharing. They failed when the EU Court ruled that such enforcement would compromise users’ privacy rights. The judgment also noted that filters would be expensive and provide little benefit to the affected businesses.

So, here in the United States, the FBI will analyze blogs, Facebook pages and Twitter streams using keyword searches. As a result, its agents will be able locate threats to our public safety and find the bad guys making them.

Groups like the Electronic Privacy Group aren’t buying. They’re calling for transparency and more oversight. And, on the face of it, that sounds fine. But, then, who would have the task of overseeing government monitoring?

Well, we could ask two tourists about the effectiveness of monitoring. Leigh Van Bryan and buddy Emily Bunting reportedly were detained by U.S. Customs for about 12 hours in a cell, interviewed by DHS officials, and then kicked out of the country after the agency put them on a one-day terrorist watch list for a tweet by Bryan that read, “Free this week for quick gossip/prep before I go and destroy America.” Because of the literal interpretation of the word “destroyed,” which, in this case simply meant partying, and another tweet about Marilyn Monroe, Bryan was charged with intending to commit a crime (weirdly, something about digging up Monroe’s grave), while Bunting was charged with hanging out with a guy who might commit a crime stateside.

You feel safer? If this one example wasn’t so funny, I might be crying about any number of our government’s recent Orwellian moves.

Regrettably, I suspect I’ll get plenty more chances. At least then I might be able to write some killin’ slang-riddled tweets.

Ilena Armstrong is VP, editorial director of SC Magazine.

“You spelled ‘confidential’ wrong.”

3M Privacy Filters offer you a crisp, clear view of your desktop computer, laptop or mobile device screen while blocking wandering eyes from seeing sensitive data. To learn why visual privacy is an important part of any data security plan, download the white paper at: 3MPrivacyFilters.com/security
Rich Baich, principal, security & privacy, Deloitte and Touche
Greg Bell, global information protection and security lead partner, KPMG
Christopher Burgess, chief security officer and president, public sector, Aliris
Jaime Chanaga, managing director, CISO Board Consulting
Rufus Connell, research director - information technology, Frost & Sullivan
Dave Cullinane, chief information security officer, eLife
Mary Ann Davidson, chief security officer, Oracle
Dennis Devlin, assistant vice president of information security and compliance services, George Washington University
Gerhard Eschelbeck, chief technology officer and senior vice president, Sophos
Gene Fredrickson, senior director, corporate information security officer, Tyc International
Maurice Hampton, technical account manager, Qualys
Paul Kurtz, partner and chief operating officer, Good Harbor Consulting
Kris Lovejoy, vice president of IT risk, office of the CIO, IBM
Tim Mathew, director, information protection, KPMG
Stephen Northcutt, president, SANS Technology Institute
Randy Sanovic, former general director, Information Security, General Motors
Howard Schmidt, cybersecurity coordinator, White House; former director, online safety technologies, Microsoft
W. Horst Tipton, executive director, (SC*)
Ariel Silverstone, former chief information security officer, Expedia
Justin Somaind, chief information security officer, Yahoo
Craig Spiezio, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft
Amit Yoran, chief executive officer, Netskope; former director, U.S. Department of Homeland Security’s National Cyber Security Division
* emeritus

Mobile security
Safeguarding handheld devices used by business execs is a challenging task—one that rarely is satisfactorily remedied. But, when it comes to implementing precautions, many companies balk with the standards, fearing the added costs. Further, while there are many who claim they’re in line, they find themselves still getting victimized by cyber criminals. Experts provide some pointers on how they are reaching a PCI-compliant state that also goes the distance in safeguarding the enterprise’s crown jewels: its data.

ON DEMAND
APTs
Some say advanced persistent threats (APTs) are a combo package of attack types complete with long-term information siphoning that can bring companies to their knees. Others, however, believe APT has become a hype-filled marketing term used by vendors to scare confused execs into buying their products. We take a look at this threat type to determine the truth.

ONLINE
Safeguarding handheld devices used by business execs is a challenging task—one that rarely is satisfactorily remedied. But, when it comes to implementing precautions, many companies balk with the standards, fearing the added costs. Further, while there are many who claim they’re in line, they find themselves still getting victimized by cyber criminals. Experts provide some pointers on how they are reaching a PCI-compliant state that also goes the distance in safeguarding the enterprise’s crown jewels: its data.

SAFEGUARDING HANDHELD DEVICES USED BY BUSINESS EXECUTIVES IS A CHALLENGING TASK—ONE THAT RARELY IS SATISFACtORY REMEDIEd. BUT, WHEN IT COMES TO IMPLEMENTING PRECAUTIONS, MANY COMPANIES BALK WITH THE STANDARDS, FEARING THE ADDED COSTS. FURTHER, WHILE THERE ARE MANY WHO CLAIM THEY’RE IN LINE, THEY FIND THEMSELVES STILL GETTING VICTIMIZED BY CYBER CRIMINALS. EXPERTS PROVIDE SOME POINTERS ON HOW THEY ARE REACHING A PCI-COMPliANT STATE THAT ALSO GOES THE DISTANCE IN SAFEGUARDING THE ENTERPRISE’S CROWN JEWELS: ITS DATA.

FOR MORE INFO
For information on SCW24/7 events, please contact Natasha Mulla at natasha.mulla@haymarketmedia.com.

For sponsorship opportunities, contact Mike Alessie at mike.alessie@haymarketmedia.com. Or visit www.scmagazine.com/scw247.

WHAT IS SCWC 24/7?
SC Magazine has created a free virtual environment that is open year-round. Each month we host an event focused on a subject that you as an IT security professional face on a regular basis.

THIS MONTH
SC WORLD CONGRESS eConference
March 20-21, 2012
eConference: PCI compliance
Unlike other standards mandating technology usage, PCI is far more specific and not open to “user interpretation.” But, when it comes to implementing precautions, many companies balk with the standards, fearing the added costs. Further, while there are many who claim they’re in line, they find themselves still getting victimized by cyber criminals. Experts provide some pointers on how they are reaching a PCI-compliant state that also goes the distance in safeguarding the enterprise’s crown jewels: its data.

ON DEMAND
APTs
Some say advanced persistent threats (APTs) are a combo package of attack types complete with long-term information siphoning that can bring companies to their knees. Others, however, believe APT has become a hype-filled marketing term used by vendors to scare confused execs into buying their products. We take a look at this threat type to determine the truth.

ONLINE
Safeguarding handheld devices used by business execs is a challenging task—one that rarely is satisfactorily remedied. But, when it comes to implementing precautions, many companies balk with the standards, fearing the added costs. Further, while there are many who claim they’re in line, they find themselves still getting victimized by cyber criminals. Experts provide some pointers on how they are reaching a PCI-compliant state that also goes the distance in safeguarding the enterprise’s crown jewels: its data.

SAFEGUARDING HANDHELD DEVICES USED BY BUSINESS EXECUTIVES IS A CHALLENGING TASK—ONE THAT RARELY IS SATISFACtORY REMEDIEd. BUT, WHEN IT COMES TO IMPLEMENTING PRECAUTIONS, MANY COMPANIES BALK WITH THE STANDARDS, FEARING THE ADDED COSTS. FURTHER, WHILE THERE ARE MANY WHO CLAIM THEY’RE IN LINE, THEY FIND THEMSELVES STILL GETTING VICTIMIZED BY CYBER CRIMINALS. EXPERTS PROVIDE SOME POINTERS ON HOW THEY ARE REACHING A PCI-COMPliANT STATE THAT ALSO GOES THE DISTANCE IN SAFEGUARDING THE ENTERPRISE’S CROWN JEWELS: ITS DATA.

FOR MORE INFO
For information on SCW24/7 events, please contact Natasha Mulla at natasha.mulla@haymarketmedia.com.

For sponsorship opportunities, contact Mike Alessie at mike.alessie@haymarketmedia.com. Or visit www.scmagazine.com/scw247.

SC MAGAZINE EDITORIAL ADVISORY BOARD 2012

Rich Baich, principal, security & privacy, Deloitte and Touche
Greg Bell, global information protection and security lead partner, KPMG
Christopher Burgess, chief security officer and president, public sector, Aliris
Jaime Chanaga, managing director, CISO Board Consulting
Rufus Connell, research director - information technology, Frost & Sullivan
Dave Cullinane, chief information security officer, eLife
Mary Ann Davidson, chief security officer, Oracle
Dennis Devlin, assistant vice president of information security and compliance services, George Washington University
Gerhard Eschelbeck, chief technology officer and senior vice president, Sophos
Gene Fredrickson, senior director, corporate information security officer, Tyc International
Maurice Hampton, technical account manager, Qualys
Paul Kurtz, partner and chief operating officer, Good Harbor Consulting
Kris Lovejoy, vice president of IT risk, office of the CIO, IBM
Tim Mathew, director, information protection, KPMG
Stephen Northcutt, president, SANS Technology Institute
Randy Sanovic, former general director, Information Security, General Motors
Howard Schmidt, cybersecurity coordinator, White House; former director, online safety technologies, Microsoft
W. Horst Tipton, executive director, (SC*)
Ariel Silverstone, former chief information security officer, Expedia
Justin Somaind, chief information security officer, Yahoo
Craig Spiezio, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft
Amit Yoran, chief executive officer, Netskope; former director, U.S. Department of Homeland Security’s National Cyber Security Division
* emeritus

WHO’S WHO AT SC MAGAZINE

EDITORIAL
VP, EDITORIAL DIRECTOR Ilona Armstrong ilona.armstrong@haymarketmedia.com
EXECUTIVE EDITOR Dan Kaplan dan.kaplan@haymarketmedia.com
MANAGING EDITOR Greg Masters greg.masters@haymarketmedia.com
SENIOR REPORTER Angela Moscaritolo angela.moscaritolo@haymarketmedia.com
TECHNOLOGY EDITOR Peter Stephenson peter.stephenson@haymarketmedia.com
SC LAB MANAGER Mike Stephenson mike.stephenson@haymarketmedia.com
DIRECTOR OF SC LAB OPERATIONS John Alban john.alban@haymarketmedia.com
SC LAB EDITORIAL ASSISTANT Judy Traub judy.taub@haymarketmedia.com
PROGRAM DIRECTOR, SC CONGRESS Eric Green eric.green@haymarketmedia.com
CONTRIBUTORS
Stephen Lawton, Bob Radliff, Jim Romeos
DESIGN AND PRODUCTION
ART DIRECTOR Brian Jackson brian.jackson@haymarketmedia.com
VP OF PRODUCTION & MANUFACTURING John Craven john.craven@haymarketmedia.com
PRODUCT MANAGER Kristian Varbamov kristian.varbamov@haymarketmedia.com
SEIC EVENTS
EVENTS DIRECTOR Natasha Mulla natasha.mulla@haymarketmedia.com
SEIC EVENTS
SEIO EVENTS
EVENTS COORDINATOR Maggie Keller maggie.keller@haymarketmedia.com

U.S. SALES
VP, SALES DIRECTOR David Soliman (646) 638-6008 david.soliman@haymarketmedia.com
WEST COAST BUSINESS MANAGER Matthew Aribon (415) 346-6460 matthew.aribon@haymarketmedia.com
SENIOR ACCOUNT MANAGER - EVENT SALES Mike Alessie (646) 638-6020 mike.alessie@haymarketmedia.com
ACCOUNT EXECUTIVE Dennis Koster (646) 638-6021 dennis.koster@haymarketmedia.com
SALES/EDITORIAL ASSISTANT Nico Howar (646) 638-6024 nic.howar@haymarketmedia.com
LICENSE & REPRINTS ACCOUNT EXECUTIVE Mukta Toure (646) 638-6031 mukta.toure@haymarketmedia.com
EMAIL LIST RENTAL
EMAIL, SENIOR ACCOUNT MANAGER Frank Cipolla, Edith Roman Associates (845) 753-3832 frank.cipolla@edithroman.com
CIRCULATION
GROUP CIRCULATION MANAGER Sherry Oommen (646) 638-6003 sherry.oommen@haymarketmedia.com
CIRCULATION SUBSCRIPTION INQUIRIES
CUSTOMER SERVICE: (800) 558-1703
EMAIL, SENIOR ACCOUNT MANAGER Frank Cipolla, Edith Roman Associates (845) 753-3832 frank.cipolla@edithroman.com

SAVE THE DATE:
SC CONGRESS
May 8-9, 2012
www.scmagazine.com/subscribe

Who’s Who at SC Magazine

Whether you are after the latest information about protecting your company’s “big data” problems, meeting ever-increasing regulatory mandates, controlling both insider and outsider attacks, or tackling other looming cyber security conundrums, SC Congress is the event for you.

This industry leading conference and expo addresses the most pressing issues with its one-day agenda, featuring sought-after industry experts sharing their experience and knowledge on everything from mobile security and cloud migration to hacktivism, APTs and the latest vectors of attack.

We hope to see you there! For more information, click on our website: www.scmagazine.com.

Exhibitor inquiries:
Mike Alessie mike.alessie@haymarketmedia.com
Marketing inquiries:
Sherry Oommen sherry.oommen@haymarketmedia.com
Program inquiries:
Illena Armstrong illena.armstrong@haymarketmedia.com

Get ready.
Get set.
We’re back.

Save the date:
SC CONGRESS
Canada
May 8-9, 2012
New York
Oct. 11, 2012
Chicago
Nov. 8, 2012

SC CONGRESS
5 • March 2012 • www.scmagazine.com
India top producer of zombie IP addresses

During the past month, the Asia-Pacific-Japan (APJ) region was the leading source of all zombie IP addresses. Of the countries making up the APJ region, India was the top producing country. For the other regions, the top producers were Uruguay in South America, the United States in North America and the Netherlands in the Europe-Middle East-Africa (EMEA) region. Source: Symantec

NEW YORK – The U.S. attorney’s office charged Bo Zhang with stealing proprietary software code from the Federal Reserve Bank of New York, where he was a contract employee. He admitted that he copied code belonging to the Government-Wide Accounting and Reporting Program for use in his private business, which trained people in programming.

BIRMINGHAM, ALA. – Chelsea Stewart, 26, was sentenced to 39 months in prison for stealing the records containing the personal data of 4,000 Trinity Medical Center patients. She had pleaded guilty to one count of wrongfully obtaining personal health information.

BELGIUM – The European Commission, the executive body of the European Union, released proposed reformations to its 17-year-old data privacy laws. Under the update, consumers would have easier access to and more control over their data, and the right to have their data deleted by a business if they request. Additionally, breached businesses would have to fess up to the EU within 24 hours.

POLAND – Hackers targeted government websites after the nation’s prime minister joined more than 20 other EU member states in signing the Anti-Counterfeiting Trade Agreement (ACTA). In response, hackers launched punishing DDoS attacks because they believe the measure infringes on their freedom of expression. Days later, Poland suspended its support of ACTA.

SINGAPORE – Two Malaysians, 27 and 39, were charged with possessing ATM skimming equipment. Authorities confiscated skimmers and PIN-hole cameras. Police believe the men are part of a transnational skimming ring that may be responsible for stealing nearly $1 million from 700 DBS Bank customers here.

PALOS VERDES ESTATES, CALIF. – Three 16-year-olds were charged with installing keylogger trojans on teachers’ computers to steal copies of future tests. They also used the malware to steal credentials for the school’s online grade system, which they accessed to change marks for themselves and others.

DALLAS – Hacker group Anonymous compromised the Texas Police Association’s website to steal and publish names, address and employment information of more than 700 officers. According to reports, the intruders were motivated by a Wylie officer who was placed on administrative lead – but not fired – while being investigated for child porn possession.

BRAZIL – Anonymous launched distributed denial-of-service attacks against the country’s largest private banks, which temporarily knocked their websites offline. The group also attacked the Sao Paulo state government and court. The hackers said the assaults were done to protest corruption and the evictions of 5,000 squatters.

IRELAND – In protest of the Emerald Isle’s version of the U.S. Stop Online Piracy Act, Anonymous launched distributed denial-of-service attacks (DDoS) against the Justice and Finance departments. The proposed copyright measure, according to critics, would favor the interests of corporations and permit the censorship of citizens.

KENYA – A hacker from Indonesia compromised more than 200 government websites, seemingly so he could redirect traffic to his blog. Using the alias Dinez, the hacker targeted the sites of a slew of ministries and other departments. All of the sites were managed by a single server, which made them all vulnerable once he gained access.
DataBank

ThreatStats

Personally identifiable data of 24 million Zappos customers was exposed

Spam  The world’s worst spam-support ISPs

<table>
<thead>
<tr>
<th>Position</th>
<th>ISP</th>
<th>Number of current known spam issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ovh.net</td>
<td>72</td>
</tr>
<tr>
<td>2</td>
<td>chinanet-zj</td>
<td>51</td>
</tr>
<tr>
<td>3</td>
<td>telefonica.com.ar</td>
<td>49</td>
</tr>
<tr>
<td>4</td>
<td>chinanet-lj</td>
<td>48</td>
</tr>
<tr>
<td>5</td>
<td>unicom-cn</td>
<td>48</td>
</tr>
<tr>
<td>6</td>
<td>hinet.net</td>
<td>45</td>
</tr>
<tr>
<td>7</td>
<td>unicom-hl</td>
<td>45</td>
</tr>
<tr>
<td>8</td>
<td>chinanet-jx</td>
<td>42</td>
</tr>
<tr>
<td>9</td>
<td>chinanet-gd</td>
<td>42</td>
</tr>
<tr>
<td>10</td>
<td>telefonica.com.br</td>
<td>41</td>
</tr>
</tbody>
</table>

The networks listed knowingly provide service to spam gangs and ignore reports from anti-spam systems and internet users. Source: www.spamhaus.org

Phishing  42 percent increase

2012 started off with a 42 percent increase in the number of attacks launched per month, as compared to Dec. 2011. As well, last month saw an increase in the total number of brands attacked. In terms of the country that endured the highest phishing volume last month, the U.K. has kept its lead for the fifth consecutive month. Source: RSA Anti-Fraud Command Center

Top breaches of the month  Data loss

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zappos.com</td>
<td>Customers were informed that their customer account information on Zappos.com may have been illegally accessed by unauthorized parties.</td>
<td>24 million</td>
</tr>
<tr>
<td>Iberdrola USA</td>
<td>A consultant contracted by the parent company of NYSERDA and R&amp;I&amp;G allowed the information systems of customers to be accessed by an unauthorized party.</td>
<td>878,000</td>
</tr>
<tr>
<td>Arizona State University</td>
<td>An encrypted file containing usernames and passwords was downloaded on Jan. 18 by an unauthorized party.</td>
<td>300,000</td>
</tr>
</tbody>
</table>

Total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005: 544,614,565 (as of Feb. 17) Source: Privacy Rights Clearinghouse (data from a service provided by DataLossDB.org, hosted by the Open Security Foundation)

Malware  Vertical encounter rate

<table>
<thead>
<tr>
<th>Position</th>
<th>ISP</th>
<th>Number of current known spam issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ovh.net</td>
<td>72</td>
</tr>
<tr>
<td>2</td>
<td>chinanet-zj</td>
<td>51</td>
</tr>
<tr>
<td>3</td>
<td>telefonica.com.ar</td>
<td>49</td>
</tr>
<tr>
<td>4</td>
<td>chinanet-lj</td>
<td>48</td>
</tr>
<tr>
<td>5</td>
<td>unicom-cn</td>
<td>48</td>
</tr>
<tr>
<td>6</td>
<td>hinet.net</td>
<td>45</td>
</tr>
<tr>
<td>7</td>
<td>unicom-hl</td>
<td>45</td>
</tr>
<tr>
<td>8</td>
<td>chinanet-jx</td>
<td>42</td>
</tr>
<tr>
<td>9</td>
<td>chinanet-gd</td>
<td>42</td>
</tr>
<tr>
<td>10</td>
<td>telefonica.com.br</td>
<td>41</td>
</tr>
</tbody>
</table>

The chart above reflects the encounter rate of web malware across a selection of industry verticals. Rates above 100 percent reflect a higher-than-median rate of encounter and rates below 100 percent reflect a lower-than-median rate. Source: Cisco ScanSafe

Spam rate  Compared to global email

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Number of current known spam issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Israel</td>
<td></td>
<td>17.01%</td>
</tr>
<tr>
<td>United States of America</td>
<td>12.03%</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td>6.31%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>2.80%</td>
<td></td>
</tr>
<tr>
<td>U.K.</td>
<td></td>
<td>2.64%</td>
</tr>
</tbody>
</table>

The chart above reflects the encounter rate of web malware across a selection of industry verticals. Rates above 100 percent reflect a higher-than-median rate of encounter and rates below 100 percent reflect a lower-than-median rate. Source: Cisco ScanSafe

Internet dangers  Top 10 threats

1. Salty.AT  Virus  2  1
2. Korga  S  Worm  0  0
3. Rehph. A  Worm  6  11
4. Fakelrean  Scarware  0  0
5. Rimecult. A  Bot  4  3
6. Hupgin  Backdoor  19  1
7. Cybot. G  Backdoor  13  5
8. Anomaly  Bot  0  0
9. Obulsaurator.XX  Malware package  3  1
10. Stref.P  Bot  20  1

Source: Trend Micro

Top 5 attacks used by U.S. hackers

1. ZeroAccess trojan
2. Butterfly bot
3. Zeus trojan
4. TDSS downloader trojan
5. Download trojan

Top 5 attacks used by foreign hackers

There were 2,163,997 attacks in the United States last month, primarily originating from Los Angeles, New York, Dallas, Phoenix and Seattle. Source: Dell SecureWorks

Zombie IPs  Global distribution

The biggest increases in month-over-month zombie activity occurred in Russia and Brazil, while the largest decreases occurred in Vietnam, China, the United States and “other” European nations. Source: Commtouch Software Online Labs

Top 5 attacks used by U.S. hackers

1. ZeroAccess trojan
2. Butterfly bot
3. Zeus trojan
4. TDSS downloader trojan
5. Download trojan

Top 5 attacks used by foreign hackers

There were 2,163,997 attacks in the United States last month, primarily originating from Los Angeles, New York, Dallas, Phoenix and Seattle. Source: Dell SecureWorks

Spam rate indicates the accumulated emails tagged as unsolicited. Source: Fortinet Threatscape Report

Received spam  Top five regions

Source: Dell SecureWorks
Listening in

Anonymous pulled off one of its most brazen hacks to date, when it compromised the email account of a law enforcement official to retrieve the dial-in details for an FBI-Scotland Yard conference call. The discussion, which the group recorded and posted online, centered on the ongoing cases of several members of Anonymous and LulzSec accused of hacking and launching denial-of-service attacks.

FOR

Debate

The attack du jour, APTs, or advanced persistent threats, are real threats.

A political storm has beset Vic Toews, the backer of a controversial law enforcement bill. Toews, the public safety minister, was threatened with violence and also had aspects of his private life exposed after introducing Bill C-30 in the House.

Bill C-30 has some wide-ranging implications. It lets the government require them to provide information about customers and includes a gag order provision that stops service providers from informing customers and includes a gag order provision that stops service providers from informing customers and includes clauses. It lets the government

AGAINST

No, the majority of threats that have been labeled recently as APTs are not significant threats, but simply mass malware (usually botnets). Industry statistics peg about six percent of all PCs in the enterprise and 25 percent at the consumer level as infected with botnet-type malware. Bot masters gain remote-control capabilities, allowing them to command PCs to search hard drives for information, intercept keystrokes to access online accounts, send spam and participate in DDoS attacks. The malware is typically installed through well-known vulnerabilities in browsers and browser plug-ins, such as Java, Adobe Reader and Flash.

Prevention is simple: Patch the OS and applications, configure them for maximum robustness, uninstall Java or restrict its use to select sites, and run the PC as a normal user without administrator privileges. Once these measures are implemented, the infection rate will drop – allowing users to focus on real APTs, which previously were next-to-impossible to detect.

THE STAT

M305

The majority of threats that have been labeled recently as APTs are not significant threats, but simply mass malware (usually botnets). Industry statistics peg about six percent of all PCs in the enterprise and 25 percent at the consumer level as infected with botnet-type malware. Bot masters gain remote-control capabilities, allowing them to command PCs to search hard drives for information, intercept keystrokes to access online accounts, send spam and participate in DDoS attacks. The malware is typically installed through well-known vulnerabilities in browsers and browser plug-ins, such as Java, Adobe Reader and Flash.

Prevention is simple: Patch the OS and applications, configure them for maximum robustness, uninstall Java or restrict its use to select sites, and run the PC as a normal user without administrator privileges. Once these measures are implemented, the infection rate will drop – allowing users to focus on real APTs, which previously were next-to-impossible to detect.

The seven suspects face a total of 357 charges, including the manufacturing and possession of credit card fraud devices, authorities said. They are believed to have installed the devices on ATMs across the greater Toronto area and skimmed card information, which was then traded in Europe, South America, the United States, South Africa and the Caribbean. Fraudulent card data was also used in Mexico, the Dominican Republic, Chile and the United States.

The alleged gang leader is 34-year-old Toronto resident Svilen Marinov, who authorities said manufactured, distributed and exported the ATM tamper devices. The Toronto Police Service has a warrant out for the arrest of another individual, along with photos of 12 other persons of interest.

Google originally offered $20,000 in prizes to researchers exposing flaws in its Chrome browser. However, the search giant pulled out and began its own contest, called Pwnium, for researchers targeting Chrome. The company upped its bounty for details of a successful zero-day exploit to as much as $60,000, with a purse total of $1 million.

Google disagreed with TippingPoint over a particular type of exploit particularly relevant to Chrome: sandbox escapes. These occur when a hacker breaks the virtual sandbox that keeps a system safe from an exploit. Google requires researchers to reveal full details of their successful exploit, whereas TippingPoint only requires them to provide information of the vulnerability that it used, so that it can code a protection in its own IDS product.

Google disagreed with TippingPoint over a particular type of exploit particularly relevant to Chrome: sandbox escapes. These occur when a hacker breaks the virtual sandbox that keeps a system safe from an exploit. Google requires researchers to reveal full details of their successful exploit, whereas TippingPoint only requires them to provide information of the vulnerability that it used, so that it can code a protection in its own IDS product.

Debate

The attack du jour, APTs, or advanced persistent threats, are real threats.

The APT knows what it wants – something of high value to the victim – and goes right after it. VeriSign’s 2011 Data Breach Investigations Report indicated that there were four million stolen records in 2010, and nearly one of 10 breaches amounted to combined efforts from external attackers and insiders.

That kind of “collaboration” sets the table for an intrusion that is advanced, persistent and very much a threat. Organizations that ignore this will leave themselves open for the resulting consequences.

THE STAT

M305

The majority of threats that have been labeled recently as APTs are not significant threats, but simply mass malware (usually botnets). Industry statistics peg about six percent of all PCs in the enterprise and 25 percent at the consumer level as infected with botnet-type malware. Bot masters gain remote-control capabilities, allowing them to command PCs to search hard drives for information, intercept keystrokes to access online accounts, send spam and participate in DDoS attacks. The malware is typically installed through well-known vulnerabilities in browsers and browser plug-ins, such as Java, Adobe Reader and Flash.

Prevention is simple: Patch the OS and applications, configure them for maximum robustness, uninstall Java or restrict its use to select sites, and run the PC as a normal user without administrator privileges. Once these measures are implemented, the infection rate will drop – allowing users to focus on real APTs, which previously were next-to-impossible to detect.

The seven suspects face a total of 357 charges, including the manufacturing and possession of credit card fraud devices, authorities said. They are believed to have installed the devices on ATMs across the greater Toronto area and skimmed card information, which was then traded in Europe, South America, the United States, South Africa and the Caribbean. Fraudulent card data was also used in Mexico, the Dominican Republic, Chile and the United States.

The alleged gang leader is 34-year-old Toronto resident Svilen Marinov, who authorities said manufactured, distributed and exported the ATM tamper devices. The Toronto Police Service has a warrant out for the arrest of another individual, along with photos of 12 other persons of interest.

Google originally offered $20,000 in prizes to researchers exposing flaws in its Chrome browser. However, the search giant pulled out and began its own contest, called Pwnium, for researchers targeting Chrome. The company upped its bounty for details of a successful zero-day exploit to as much as $60,000, with a purse total of $1 million.

Google disagreed with TippingPoint over a particular type of exploit particularly relevant to Chrome: sandbox escapes. These occur when a hacker breaks the virtual sandbox that keeps a system safe from an exploit. Google requires researchers to reveal full details of their successful exploit, whereas TippingPoint only requires them to provide information of the vulnerability that it used, so that it can code a protection in its own IDS product.

Google disagreed with TippingPoint over a particular type of exploit particularly relevant to Chrome: sandbox escapes. These occur when a hacker breaks the virtual sandbox that keeps a system safe from an exploit. Google requires researchers to reveal full details of their successful exploit, whereas TippingPoint only requires them to provide information of the vulnerability that it used, so that it can code a protection in its own IDS product.

Debate

The attack du jour, APTs, or advanced persistent threats, are real threats.

The APT knows what it wants – something of high value to the victim – and goes right after it. VeriSign’s 2011 Data Breach Investigations Report indicated that there were four million stolen records in 2010, and nearly one of 10 breaches amounted to combined efforts from external attackers and insiders.

That kind of “collaboration” sets the table for an intrusion that is advanced, persistent and very much a threat. Organizations that ignore this will leave themselves open for the resulting consequences.

THE STAT

M305

The majority of threats that have been labeled recently as APTs are not significant threats, but simply mass malware (usually botnets). Industry statistics peg about six percent of all PCs in the enterprise and 25 percent at the consumer level as infected with botnet-type malware. Bot masters gain remote-control capabilities, allowing them to command PCs to search hard drives for information, intercept keystrokes to access online accounts, send spam and participate in DDoS attacks. The malware is typically installed through well-known vulnerabilities in browsers and browser plug-ins, such as Java, Adobe Reader and Flash.

Prevention is simple: Patch the OS and applications, configure them for maximum robustness, uninstall Java or restrict its use to select sites, and run the PC as a normal user without administrator privileges. Once these measures are implemented, the infection rate will drop – allowing users to focus on real APTs, which previously were next-to-impossible to detect.

The seven suspects face a total of 357 charges, including the manufacturing and possession of credit card fraud devices, authorities said. They are believed to have installed the devices on ATMs across the greater Toronto area and skimmed card information, which was then traded in Europe, South America, the United States, South Africa and the Caribbean. Fraudulent card data was also used in Mexico, the Dominican Republic, Chile and the United States.

The alleged gang leader is 34-year-old Toronto resident Svilen Marinov, who authorities said manufactured, distributed and exported the ATM tamper devices. The Toronto Police Service has a warrant out for the arrest of another individual, along with photos of 12 other persons of interest.

Google originally offered $20,000 in prizes to researchers exposing flaws in its Chrome browser. However, the search giant pulled out and began its own contest, called Pwnium, for researchers targeting Chrome. The company upped its bounty for details of a successful zero-day exploit to as much as $60,000, with a purse total of $1 million.

Google disagreed with TippingPoint over a particular type of exploit particularly relevant to Chrome: sandbox escapes. These occur when a hacker breaks the virtual sandbox that keeps a system safe from an exploit. Google requires researchers to reveal full details of their successful exploit, whereas TippingPoint only requires them to provide information of the vulnerability that it used, so that it can code a protection in its own IDS product.
Perhaps no single reported breach in recent memory better highlighted the risk that vulnerable third parties present than when hackers last year raided the systems of marketing services firm Epsilon. The intruders plundered a massive amount of data — tens of millions of email addresses — belonging to customers of big-name clients served by Epsilon. The incident underscored the sheer amount of trust that businesses place in companies that maintain their data, not to mention those vendors that provide system and application development, support and maintenance.

“Due to a customer, whether or not you contracted with, it’s you who lost the data,” said Daniel Kennedy, a former CISO who now is research director of information security and networking at The 451 Group.

Considering the widening attack surface and the increasing number of partner relationships, guidance and laws are beginning to emerge. As of March 1, the Massachusetts data security law’s grandfather provision expires, which means that any contract — regardless of when it was signed — must include language binding third-party service providers to protect personal information.

Of course, one cannot rely on a law or contract alone to ensure that sensitive data shared with a partner will be protected. Many organizations opt to conduct annual risk audits, but often they merely present a snapshot-in-time overview of a third-party’s security stance. When deciding on whom to do business with, businesses traditionally roll the dice. “The third party is only going to agree to certain things in the contract negotiations,” Kennedy said.

But a company called Saperix, which was acquired last year by FireMon, wants to apply a metric to the decision-making process. In January, Saperix received a $500,000 grant from the National Science Foundation to develop a service that rates the information security risk of businesses, much like currently exists with credit scores.

69% of health care organizations have “little to no confidence” in their business associates’ ability to protect sensitive data.

Source PwC PINNOM Institute/ID Experts

JOBS MARKET
Me and my job

Seth Bromberger
EVP of information sharing and government programs for the Energy Sector Coordinating Council

Why did you get into IT security?
I liked the idea of working to keep the bad guys out of things. I also enjoy learning about the really novel, creative ways bad guys have discovered to circumvent security controls. Studying the offense gives me a better understanding and appreciation of defense and, for me, it never gets stale.

How do you describe your job to average people?
Most of my job right now is focused on ensuring that the people who are responsible for protecting critical infrastructure, particularly in the electric sector, have the information they need to do their jobs effectively.

What was one of your biggest challenges?
It’s a continuing challenge: figuring out how to provide security for emerging technologies within our critical infrastructure.

What keeps you up at night?
I know we have really good folks working on this problem set, and losing sleep would make me less effective.

Of what are you most proud?
I’m proud of the dedication I see among my colleagues who are in critical infrastructure security. I’m proud of the way we’ve come together to share and help each other within the utility space. I’m also proud of the projects I’ve been involved in — from helping develop our industry information-sharing organization to my role in creating the first situational awareness system for monitoring anomalous security events, and correlating those events with malicious activity.

For what would you use a magic IT security wand?
I’d use it to find the balance between confidentiality and openness. I believe that security is often used not just as a means to deny access to information that is not sensitive, but where it’s easier or more politically expedient just to say “no.” This misuse destroys trust, making it harder to apply controls in cases where their use is legitimate.

Chris Ray, chief information security officer, Epsilon

Chris Ray, chief information security officer, Epsilon

Chris Ray, chief information security officer, Epsilon

Expertise: Calif.-based provider Voltage Security, a provider of data-centric encryption and key management, has partnered with Paris-based Ingenico, a provider of payment solutions, to combat card fraud via encryption at the point-of-sale.

www.voltage.com
www.ingenico.com

Dallas-based Epsilon, a marketing services firm that sustained a massive breach last year, has announced the appointment of two security industry veterans to its team. Keith Morrow has joined as EVP and chief information officer, and Chris Ray has joined as chief information security officer. Morrow, formerly CIO at Blockbuster and 7-Eleven, will be responsible for the company’s global IT structure, overseeing more than 200 technology pros, while Ray will have enterprise responsibility for information security and regulatory compliance. This is the first time Epsilon has filled these positions.

www.epsilon.com

John Strofert, former CISO and deputy chief information officer for information assurance at the U.S. Department of State, has taken a new position as director of the National Cyber Security Division at the U.S. Department of Homeland Security. He will be working on similar project initiatives at his new post.

www.dhs.gov

Seth Bromberger, director of Solutionary Engineering Research Team (SERT) Information Technology Sector Coordinating Council (IT SCC). He has been serving as vice chairman at the council, which works on behalf of companies and associations in the IT industry to coordinate initiatives and to lobby, on behalf of the sector, for infrastructure protection, response and recovery. IT SCC works with ISACs in public-private partnerships under the Department of Homeland Security’s National Infrastructure Protection Plan.

www.isalliance.org, www.it-scc.org

Seth Bromberger, director of Solutionary Engineering Research Team (SERT)

www.epsilon.com

Information Technology Sector Coordinating Council (IT SCC).

Rob Kraus, director of Solutionary Engineering Research Team (SERT)

Seth Bromberger, director of Solutionary Engineering Research Team (SERT)

Seth Bromberger, director of Solutionary Engineering Research Team (SERT)

Seth Bromberger, director of Solutionary Engineering Research Team (SERT)

Seth Bromberger, director of Solutionary Engineering Research Team (SERT)

Seth Bromberger, director of Solutionary Engineering Research Team (SERT)
Protect data on the go

Over all, the exploding use of smart mobile devices and the business productivity that accompanies this trend is a wonderful thing. However, it has many CIOs and IT administrators reeling. They are constantly asking themselves, “Do I really know where our sensitive data is and is it safe?”

This concern is not unfounded. Plenty of their critical corporate data is likely going places never even imagined – in a bar or coffee shop, wandering the streets, maybe even into the hands of a stranger. Wherever employees are toting their smartphones and tablets, chances are they are also carrying sensitive information.

The answer, however, is not to prevent the use of these new and innovative mobile devices. Instead, a new goal has to be made: securing information no matter where it goes.

Therefore, what enterprises must do is extend their mobile security strategies – which hopefully already take mobile device management and endpoint security into account – to include encryption policies. By thus securing data itself, the risk of losing sensitive information can be greatly reduced. Imagine for a moment an attacker has gotten their hands on an employee’s smartphone. By either guessing a too-simple screen-lock password or using software to crack it, this miscreant now has unfettered access to the employee’s email and all the sensitive information therein. However, if encryption had been employed, the messages in the employee’s inbox would have remained inaccessible.

In short, it has grown impossible for organizations to know everywhere their potentially sensitive data will go. The interconnected nature of the web, the amount of sensitive information and the ease of access enable hackers to take a data breach at one company and commit fraud on a multi-national scale.

Websites must make strong authentication standards a priority.

The password is dead

The massive fallout from the breaches of Gawker, Sony and others involving weak password authentication schemes show that the current password system is dead. Let’s face it: People can’t remember the complex passwords needed for secure logins – not when they have an average of 25 online accounts, and growing. It’s time we recognize that this system is not sustainable or secure.

New forms of authentication must emerge. Many organizations lay the burden of secure authentication at the feet of users, who have proven time and again that their nature is to choose weak passwords and use the same password for multiple online accounts. Rather than telling people to remember ever more complicated strings of letters, numbers and symbols, businesses need to adopt new authentication approaches that are more secure and easier on people.

The interconnected nature of the web, the domino effect of poor password practices, and the amount of sensitive information shared and stored online means that the burden needs to shift. Websites must make strong authentication standards a priority.

The availability of cloud-based authentication solutions make it easy for websites to employ one-time passcodes for logins, which can replace traditional passwords completely or be added to strengthen the security of the login if the user has a weak password.

As well, the widespread use of mobile phones makes it possible for websites to employ multifactor authentication without using tokens, smart cards or biometrics. Additionally, image-based authentication provides yet another way for organizations to offer an easier, yet more secure form of authentication.

Until more websites eliminate “dead” password schemes in favor of strong authentication methods that are easy for users, we’ll continue to see poor password practices, enabling hackers to take a data breach at one website and use the revealed credentials to compromise accounts and commit fraud on a number of other websites.

Defining a DLP strategy

Jeffrey Brown, global information security program manager, GE Capital

Data leakage prevention (DLP) solutions remain fairly immature, but the need to protect and monitor sensitive information is greater than ever. Creating a coherent DLP strategy can seem challenging, but it all starts with understanding the business requirements.

Start by answering the fundamental questions. Is your organization looking to achieve basic regulatory compliance, or understand how sensitive data is being used and where it is being accessed? Do you want to actively block sensitive data, filter it or just monitor it? You need to consider all these scenarios in the context of data at rest, in transit and in use.

These requirements will ultimately be translated into DLP event triggers, so engage your business early on in this process. If you are deploying a global solution, you may also need to factor in employee privacy issues. While you should always start with meeting basic compliance requirements, the most value will come from bringing your business leaders to the table. Many DLP tools come with basic predefined policies addressing things like sensitive personally identifiable information, but what does intellectual property look like in your organization, and what should be done when these assets fall outside the parameters of acceptable use?

A key decision point will be deploying a gateway or endpoint monitoring solution. DLP endpoint monitoring tends to be more sophisticated, but can introduce support headaches. Endpoint monitoring solutions also tend to focus on Windows PCs, often neglecting mobile platforms, Linux and Mac. The “bring-your-own-device” trend will introduce a whole new breed of monitoring challenges at the endpoint. Gateway solutions tend to be broader in their reach, but may be less sophisticated in their ability to respond to events.

If you need fine-grained control over how users print and access USB ports, then you need to focus on the endpoint. If broader response controls are acceptable, a gateway solution may make more sense. Ultimately, a hybrid approach may be your best choice.

Event response should be automated wherever possible. The output of these tools can be significant, and you won’t be able to hire enough analysts to pore through all the data manually. Distinguishing between priority events that need a more formal response and low-level events that can be automated will be critical.

Start small and keep aggressive control over your project scope. Most DLP deployments are multiyear efforts that will evolve over time. And don’t neglect the basics. Simple steps, like ensuring your laptops are encrypted and user awareness programs are up to date, can also serve as components of a solid strategy.

30 seconds on...

> User education is key

A strong DLP program addresses user education, says Brown. It’s not enough to simply block or monitor sensitive data. Make sure that users understand the security policy.

> Tools to simplify tasks

Also, provide them with compliance tools, like email encryption. Many DLP tools are even capable of automatically enforcing requirements, like data encryption.

> Spread the word

You will need to work with leaders across the company, as well as employees. DLP should be an education and awareness exercise as much as it is a means of protecting data.

> Nothing is foolproof, but...\n
Of course, no DLP solution will prevent a determined and intelligent insider, but don’t underestimate how many exfiltration incidents occur by mistake every year.
Disciplines like philosophy or history fail to conjure up images of the stereotypical information security professional in the mind’s eye. Backgrounds like this, though, have spawned some immensely inventive and often accomplished chief security officers over the years.

In fact, according to many experts, the IT security market largely has been formed on the backs of individuals from various branches of learning. It’s because of these diverse experiences and wide-ranging credentials that the field has been so energizing to the many professionals who have fostered its continued growth and current entrance into the mainstream.

“Dan Geer made a great observation when he said that the makeup of the people in our profession is dramatically shifting,” explains Stephen Scharf, global CISO of Experian, and SC Magazine’s 2012 CSO of the Year award winner, which is announced each year at the SC Awards U.S. gala in February. “Fifteen years ago, people got into security from a different field. This was very exciting because they brought their existing skill sets when solving problems. So when you put together a network engineer, a Windows engineer, a lawyer, a programmer, a biostatistician and a kid from the NSA to solve a problem, you get some really creative solutions. That is starting to shift as more security folks are entering the industry directly from college.”

Scharf admittedly joined the profession via the old-school approach. “My mother offered me some great advice when I was struggling with what to pick as a major,” he says. “She said that whatever you major in will not define your lifelong profession. So, instead of stressing about what you want to be, it is better for you to declare a major that you enjoy and [from which you] will learn something.”

Learning is an activity Scharf engages in everyday, says his friend and industry peer Dave Cullinane, CSO and vice president of eBay, and SC Magazine’s CSO of the Year in 2005. “He’s a quick study, just brilliant,” says Cullinane, adding that once Scharf has a sound understanding of a subject area, he’s quick to use the knowledge in inventive ways to improve situations—often without disruption to others. “He’s a really good student of the profession.”

Right after college, Scharf was a sales representative for Generative N/C Technology, a small company where he did sales, customer support and even ran the...
company’s trade show presence. “That is where I cut my teeth on technology and got excited about it,” he says. It was among various areas of interest for Scharf in his younger days. “I have always been someone who likes to tinkern and [I tend to] focus on things that are logical and analytical,” he says. “This is why technology has always appealed to me.”

After getting a taste for the industry at Generative, Scharf went on to work as a systems and network engineer for a bank, moved over to a server group manager for a lab, and then took a senior security consulting gig at the well-known professional services company @Stake where he was CTO.

Dave Aitel, a National Security Agency research scientist at age 18, who moved on to @Stake six years later where he also worked as a senior security consultant, says Scharf is an anomaly. As he honed both his technical and policy knowledge, he flourished as a consultant. The overarching requirement to teach executive clients how to partner with corporate goals further bolstered a natural transition to the CSO role.

“He has a cool head,” says Aitel, adding that is key to managing multimillion dollar risks to the business. “You can’t be excitable in (the CSO) post. It’s a marathon. Stephen’s not thirsty. If you’re too thirsty, you wouldn’t last two weeks,” he says.

It was in 2002 that Aitel left @Stake to launch Immunity, a software security company, where he is now CTO. Around that time, Scharf moved on to financial news corporation Bloomberg where he worked for Aitel’s wife, who was CSO at the time. Later, he took over the post.

“He knows from Bloomberg that it’s not a thankless job,” says Aitel. “People don’t come up to you and say, ‘Hey, good job on stopping all those attacks.’ They only come to you when something bad happens. There’s no positive feedback to that job — only negative. So it takes a special brain to say, ‘I’m doing a good job. I know it internally. I don’t have to have external feedback on that.’”

Such intrinsic drive likely came in handy as Scharf moved to his current post at Experian, where he’s done much to strengthen the company’s overall information security and compliance posture, says his boss Robert Nelson, global general counsel.

“Stephen was hired to lead the globalization of our information security program,” says Nelson. “His leadership has provided for consistent security practices across the organization and resulted in increased resiliency in our infrastructure.”

In addition, Scharf also has had a hand in ensuring that the company’s own product offerings are sound, adds Nelson. “By helping to identify and reduce risk during the product lifecycle, Stephen has supported our growth strategies by ensuring the deployment of appropriate controls.”

As a company that generated $4.2 billion in revenue during its last fiscal year, this is no small feat. Experian has operations in 41 countries and employs 15,000 people.

“Through a robust collection of partners, resellers and direct subscribers, we provide data products which enable our clients to make critical financial decisions,” explains Nelson. “We also offer many direct-to-consumer products that provide assistance with credit monitoring and identity protection.”

Scharf’s role in helping to maintain the company’s internal controls and safeguarding the integrity of its solutions is critical and requires the combination of technical prowess and business acumen. Armed with these traits, strong CSOs can help leaders understand and support any IT security necessities that are required to run successful organizations in today’s technological world.

“Stephen is able to translate security requirements from technical speak into business drivers,” says Nelson. “Before Stephen joined Experian, we had a ‘stopgap’ approach to information security. Each region operated successfully, but leveraged different methods. By globalizing the program, we have been able to elevate the best practices in each region into our global standard.”

Immunity’s Aitel puts it more directly: “Previous to Stephen, they were getting hacked and, now, not so much.”

And while the company probably will one day find itself victimized by cyber criminals — after all, “no one plays perfect ball” — Scharf, who, remember, is very clear-headed and calm, thinks long-term, adds Aitel. These attributes combined with his in-depth and varied experiences will serve any company well today.

When Scharf was at Bloomberg in New York as the company’s information security lead, he was subsequently assigned the task of overseeing the physical security side of the house. A little taken aback and a tad bit stressed by this addition to his duties since it was a space with which he had little experience, Scharf still was underwhelmed by the challenge. But, he needed some mentoring and guidance in this area, so he turned to Cullinane, who was working for a financial institution in Massachusetts at the time and had oversight of IT and physical security. Spending “a bunch of time” with his friend and the security team in New England, Scharf proved in a quick study, says Cullinane. He became one of the most innovative pros at the time, marrying physical and IT security requirements to establish a balanced risk perspective by putting “bleeding-edge” controls in place.

“He’s done an extraordinary job,” says Cullinane. “He looks at things and tries to think of better ways to solve problems. He’s absolutely one of the best in the business.”

The various practices he’s put into place at Experian seem to bolster the compliment.

“Stephen is focused on helping to ensure our security strategy matches closely with our business objectives,” says his boss Nelson. “He routinely meets with senior leadership to understand their goals and adapts our security initiatives as needed to reduce areas of risk. Our security program continues to evolve, and enhancements are always taking place where measurable improvements can be gained.”

For his part, Scharf says he never regretted opting for humanities over science in college.

“When I feel that a humanities background gives you core skills in writing, literature, history, philosophy and psychology that transcend any profession,” he says. “I cannot tell you how many computer science majors I have met that still cannot write a grammatically correct email, or reference historical facts and figures.”

At the same time, given the huge growth of undergraduate and graduate programs offering concentrations in information security, Scharf wonders if his current field’s future.

“It will be interesting to see if the level of creativity diminishes as a result of the lack of other perspectives,” he says.

Scharf also offered his perspective on other areas near and dear to CSOs.

Illena Armstrong: How long have you been in information security in your current role? Stephen Scharf: I have worked in information security for the last 14 years. Before working in the field, I held various positions in information technology, customer service and sales. I believe that having a background in IT operations allows me to better understand the impact of security actions/strategies. I also believe that having previous experience in sales and customer support has allowed me to better communicate with business leaders while focusing on client growth and satisfaction.

IA: What were the major challenges you face daily? SS: By focusing on consistency in operations, we have also been able to demonstrate measurable cost savings. By reducing complexity we have been able to consolidate some vendor relationships and thus drive down unit costs due to higher volumes. We have also justified increased automation in some areas by articulating the reduction in manual intervention. For example, PC infections waste valuable time for both the affected employee and the help desk. By reducing infections we also can reduce the amount of wasted personnel hours, and justify the cost of a preventative solution.

IA: In your organization, have you been able to leverage all these achievements? SS: Help is offered from many areas. First off, we have a great security team

CSO of the year
that continually converts strong ideas into actions. We then partner with sourcing and [the] supply chain to vet through vendor solutions and evaluate third-party security controls. We then partner with our IT organization to effectively roll out technical solutions. We then partner with FBI and legal to ensure that appropriate policies are crafted to drive employee behavior.

IA: What processes and vendors helped you reach your project goals?

SS: We have partnered with multiple vendors which supply hardware, software and consulting services. We reduce our complexity by limiting the number of vendors we leverage, but at the same time we are conscious of not falling into the trap of monoculture. We leverage dissimilar solutions/vendors when appropriate to ensure that a single gap is not propagated extensively.

IA: How about Experian’s own solutions? SS: Experian sees the security and privacy of data as a critical component of its strategy as one of its highest priorities. We have a vast collection of internal practices, as well as a comprehensive set of security policies, that we leverage. We routinely participate in client audits, and walk our customers through our practices. We also have completed our sixth year of PCI certification for our products and services that touch credit card data.

IA: Is this a sign that more companies and individuals care more about how organizations are shepherding their critical content?

SS: Absolutely. The concept of “trust, but verify” has quickly replaced trust and verify” has quickly replaced trust and does not always branch out toward other data-related risks.

IA: Do you foresee budgetary challenges?

SS: The past few years has required all organizations to reflect on their operational costs and see where improvements could be made. Experian maintains a practice of being fiscally sound in its approach and ensures appropriate value for services. This has not resulted in a direct drop in security spend.

IA: Must you contend not only with regulations in the United States, but also with other countries’ regulations?

SS: We operate in multiple countries and partner with our internal compliance and legal departments to correctly define and support adherence to applicable laws and regulations.

IA: How do privacy issues factor into what you do?

SS: Privacy of data is a critical component of our governance programs. Each new product/service must pass through a series of legal and compliance reviews to ensure that data is used in accordance with our privacy policies, in addition to industry regulations.

IA: What advice would you give to others looking to enter the field of information security?

SS: I work closely with our privacy team as they address the many external requirements that are relevant to our global operations. Some of the items we follow are HIPAA, PCI, GLBA, FISMA, as well as EU data protection requirements.

IA: What advice would you give to individuals looking to enter the field of information security?

SS: Great people are always hard to find and in high demand. When looking at candidates, I focus more on experience and results than on certification and degrees. What have you accomplished and how creative you can be is a greater draw than an acronym after a name. For new individuals entering the field, I would suggest they get some complementary skills to add to its IT security. Having some operational experience is always a plus. This way you have a better understanding of the impact of your security recommendations.

IA: What is on your future agenda?

SS: Experian has a history of growth via acquisition. Activities next year will focus on the continued integration of our acquired entities, as well as a myriad of continual improvements across our application and network infrastructure.

IA: What other specific projects are on tap for this year and starting in the next?

SS: We continue to dedicate time and money toward our information security awareness campaigns. Our team is able to use an appropriate amount of humor in order to deliver entertaining content, while still handling the material in a respectful way.

IA: What about the major threats to your organization and its critical data?

SS: Employee diligence is an ongoing effort. As previously mentioned, we spend considerable time and money on employee awareness. We understand that employees are focused on getting their jobs done and do not always think before clicking. Therefore, we marry our awareness efforts with numerous automated protections to help deter the risk of malicious activity initiated by user behavior.

IA: What are the threats/newer applications that you think you and others in your position must address this year?

SS: I do not foresee a new class of attacks, but rather continued sophistication of existing attack vectors. I believe that malicious events will continue in the same frequency and leverage greater use of stealth. The obvious signs of the ‘Nigerian scam’ messages will be replaced with phishing and other social threats that prey on the average user. The continued proliferation of data breaches will aid in fostering these attack vectors and lead to an increased success rate.

IA: What is the security technology that you leverage which could be of most benefit to organizations?

SS: There is no one-size-fits-all solution. Organizations must address this year?

SS: We have grown past the basic use of firewalls and anti-virus. Those are now defined as the preschool requirement of the information security professional. More robust security programs will leverage a mixture of DLP solutions, malware detection, application-level firewalls and forensic tools.

IA: What about policies and programs?

SS: These are a must-have in any organization. The security policy defines what is acceptable. It is then possible to leverage policies to establish control baselines, which are measured across the organization.

IA: What's your best advice to others when it comes to building a strong security program?

SS: The first thing I'd say is make sure that your security strategy maps successfully to your company's risk profile. Security is highly subjective and can be ultra-conservative, such as top-secret government installations, or it can be loose and flexible, like a new start-up. As a successful security executive must understand the appropriate level of risk in their organization and then build their security program to complement that risk level.

IA: Any hobbies, destination spots or other personal areas of your background that you would like to share?

SS: That's a good question. I recently started to pick up golf and enjoy a good game of poker or chess. I also volunteer in the industry and currently sit on the board of directors for ASIS [a security organization with 37,000 members worldwide that develops educational programs]. I am also a past member of the board of directors for the Information Security Systems Association [ISSA, a nonprofit, global organization of information security professionals and practitioners].
Could Canada be a haven for companies nervous about cloud storage in the United States? It needs to shape up first, reports Danny Bradbury.

Canada has never been a leader in computing. Outside of a few companies, like Nortel and RIM (both of which have seen better days), it has been a follower. But, could its cloud computing industry be different, capitalising on concerns over privacy and government scrutiny in the United States?

Wally Kowal, founder of Canadian Cloud Computing, a Kitchener, Ontario-based hosting services company, envisions three different types of customers seeking hosting arrangements. The first are Canadian firms with a specific legal requirement. For example, organizations in the health sector have to know exactly where their data is residing. And, public sector organisations based in Nova Scotia and British Columbia are limited in their outsourcing options when it comes to cloud computing.

The second tier of customer has a regulatory requirement. “In that case, there is no law saying that they have to keep their data in Canada, but they’ve identified it as best practice,” Kowal says. Businesses in the insurance industry are a good example.

Finally, some customers rest easier knowing that their information is stored north of the border. But, why would they feel that way? Mostly, it’s to do with the legislative landscape in the United States.

U.S. law contains measures that allow authorities to gain easy access to private information without a warrant, and these laws also forbid record-holders to tell the subject about the subpoena. This can be carried out using National Security Letters (NSLs), which are documents issuable by FBI field agents. As well, the USA Patriot Act, passed in Oct. 2001, in the days following the Sept. 11 attacks, expanded the conditions under which NSLs could be used. Although, two lower federal courts found NSLs to be constitutionally questionable, their use continues today, albeit somewhat modified under the USA Patriot Improvement and Reauthorization Act of 2005.

So, while some restraints have been imposed, U.S. investigators can still access IP addresses, email addresses, logon times, lengths of service and billing records, and section 215 of the Patriot Act allows authorities to ask for information about “any tangible thing,” including books, documents and other records, with little, if any, proof that it is needed, using what’s known as a business record order (BRO). This decree also comes with a gag order that stops the cloud computing provider from informing the target. And, add to that the fact that the FBI seems to be requesting more internet-based information from providers than ever before. A report in the Washington Post found that 80 percent of requests filed via BROs were for internet-based information. According to the Justice Department, the number of BRO requests filed by the FBI in 2010 more than quadrupled over 2009.

Some believe that this snooping option will scare customers enough to go north of the border. Milan Vrecic, founder of Nova Scotia-based file-sharing company TitanFile, invested heavily in the creation of a Canadian cloud service just for this purpose.

“We have U.S. universities as clients who store files on our Canadian servers,” he says. “When we talked to them, the biggest reason was the Patriot Act.”

Kowal adds that he has been approached by India-based outsourcing companies. Most of the potential clients there have spoken to were sent by request of their Canadian customers. “The company can’t open up a whole new Canadian division, so they contact us and say, ‘Can you build this for us?’”

But does storing cloud data on servers based in Canada really provide advantages to global customers? Several commentators think not.

“Almost every single civilized country has something similar to the Patriot Act,” says Francoise Gilbert, a privacy and security attorney with a special focus on cloud computing.

“In the United States, it is actually better. It is more regulated. There are rules and processes. If the government wants access to something, it has to go through certain steps.”

And Canada already has several laws that allow the government to access information, Gilbert says, citing the Security Intelligence Service Act, which allows judges to issue warrants authorizing the interception of communication.

As amended in November 2001, Canada’s National Defence Act also permits the so-called communications security establishment to intercept transmissions for foreign intelligence purposes under Section 273.65. And the Personal Information Protection and Electronic Documents Act (PIPEDA) also allows, for investigative purposes, the collection and use of personal information without the knowledge or consent of an individual.

Pending legislation in Canada promises to make the country even more U.S.-like in its surveillance powers. Bill C-12 would clarify that a party making a request under PIPEDA would not need a warrant. It would require only “lawful authority,” a term which is itself unclear, and which many service providers will take to mean “requested by a police officer.”

As well, the highly contentious Bill C-30 reintroduces the lawful access measures that, owing to the early Canadian election, died on the ballot last year. As currently written, this legislation would effectively give the Canadian government complete control of an ISP’s networks and systems, thanks to a provision that lets the government stipulate the exact nature of the surveillance equipment that would be installed.

In any case, simply holding data in Canada doesn’t guarantee immunity. “If you operate in the U.S., there’s a legal right to have access to that data, and there’s a precedent around that,” says Gord Smith, partner at Canadian IT consulting firm Idefac. “The data is accessible if you operate in the U.S., period.”

There are also mutual legal assistance treaties, Gilbert says. Many countries take advantage of these regularly to exchange information. “So there is concern, but it is due in large part because of misinformation,” he says.

On the other hand, those companies doing business in Canada without U.S. offices may still find themselves at an advantage, shielding their data from the scrutiny of at least one government by storing it in Canada. And storing it in Canada rather than some other locale carries an additional benefit: proximity. This can be a big factor, says Richard Davies, CEO of ElasticHosts, a cloud services company with data centers in the United States, Europe and Canada.

“We’ve seen many European customers of ours saying that they want a North American site because putting their web application out is a bit slow for North American customers,” he says. “When they look at our three localities, they say that Toronto is a reasonable choice.”

Storing data on Canadian servers may not offer as many privacy benefits as companies might have hoped, though, says Kowal. Canada could make the advantages clearer if it were a little less draconian in its own legislation.

“If we had well-written, understandable and reasonable laws, we could very well become the Swiss bank of data,” he says.

Canada offers proximity, a robust technical infrastructure and a politically and economically stable climate that makes it perfect for near-shoring data storage, industry observers say. If only it could differentiate itself a little more, legally, it could be in pole position to provide cloud-based services.

But those myriad challenges are political, not technical — and there’s no app for that.
In fact, the FBI and Scotland Yard fell victim to those that they were hunting down when Anonymous posted on the internet a 16-minute conference call it purloined between the two agencies.

“Law enforcement’s efforts have had little real effect on curbing hacktivism since it operates at a scale of anonymity and ease that current governments and their laws are incapable of comprehensively acting on,” says Phil Lieberman, president of Lieberman Software in Los Angeles. Hacktivism, he adds, is on the increase as the world becomes more and more connected, with a proportional number of weakly secured systems available for exploitation.

Despite devoting resources and making arrests, authorities seem little closer to stopping the new face of social protest, reports Jim Romeo.
AN EDUCATED DECISION

West Virginia University was looking to protect student and staff data... and it found a solution, reports Greg Masters.

When West Virginia University (WVU) was established in 1867 along the banks of the Monongahela River, the patent filing for the telephone was still a decade away. IBM’s big data shipping messages took some time. Fast forward about 150 years, and WVU was facing another challenge with its communications, but this time it was a massive increase in the amount of data moving across its network.

The institution has come a long way from its earliest days as an agricultural college, assembled on the foundation of two former academies and a woman’s seminary and nestled on land that had once been hotly contested among early settlers, British and French military and Native Americans. Now, along with Morgantown Personal Rapid Transit system, a monorail that connects WVU’s three Morgantown campuses with the downtown area, systems are needed as well to transfer data of the institute’s growing population. For its fall 2011 semester, around 33,000 students enrolled. Add to that approximately 6,500 faculty and staff on the main campus in Morgantown, as well as spread across several regional campuses in Montgomery and Keyser, and that’s a lot of personally identifiable information (PII) to protect.

With the ever-increasing threat landscape and new attacks being launched daily, Alex Jalso, assistant director in the Office of Information Security at WVU, needed to ensure that web applications, either developed in-house or purchased from vendors, did not have vulnerabilities that would put the university at risk. It was time to transition from a reactive to a proactive approach, he says.

“AppScan uses static or white box analysis to scan source code or byte code directly, allowing detailed analysis of potential taint flow and identification of issues pinpointed to the precise line of code,” says Jack Danahy, security executive at IBM Rational. “The tool also uses dynamic or black box analysis to analyze complete web applications by automatically crawling the code, mutating server requests and analyzing responses, he says. Further, new JavaScript analyzer capabilities allow AppScan to study client-side JavaScript for potential vulnerabilities, allowing it to identify security flaws that have been overlooked by other tools. And, the latest version of AppScan has added run-time, or glass box, analysis, which monitors apps during a dynamic scan to enhance test coverage.

A noticeable benefit is that the tool integrates with software development lifecycle tools, allowing teams to make security testing part of their process rather than an expensive afterthought.”

Implementation smooth

With the assistance of IBM’s AppScan Enterprise (ASE) support staff, the deployment of the tool across the enterprise went smoothly, Jalso says. And, he appreciates how easy it is to manage.

“Our IBM team has filed many patents, including runtime analysis and the first and broadest patent on web application security scanning issued in 2003,” he says. “Our AppScan team has focused on making application security fit into the development environment and the security infrastructure in organizations, says Danahy. IBM AppScan products are complemented by the IBM Security framework that includes offerings specific to threat mitigation on the network (IBM Security Network IPS), for servers (IBM Security Server Protection) and for databases (IBM Infosphere Guardium), Danahy says.

BIG BLUE: New resources

The IBM team of application security experts has led research in this area for 14 years, says Jack Danahy, security executive of IBM Rational. Before arriving at IBM, Danahy was founder and CEO of two technology companies: Qiave Technologies, sold to Watchguard Technologies in 2000, and Dunce Labs, sold to IBM in July of 2009. As well, Danahy served on the board of the Payment Card Industry (PCI) Vendor Alliance, and is a distinguished fellow at the Ponemon Institute.

In addition to running the university’s data network, WVU’s security team conducts online webinars, workshops and classes to teach computer best practices to students and staff.
Applications are anything but static. They may start out with one set of functions, then elements are added on and merged with other applications. As they grow more complex, their vulnerability density increases – a particular problem for applications hosted on the web and migrating to the cloud.

“Web applications are the top attack target because they’re so difficult to protect,” says Jim Manico, volunteer connections committee chairman for the Open Web Application Security Project (OWASP), and vice president of security architecture for WhiteHat Security. “Today, cloud deployment is all web driven, meaning cloud and web application vulnerabilities are on a direct collision course.”

Developing a “secure-by-design” framework for these technologies is challenging enough; says Michael Coates, volunteer OWASP chairman and director of security assurance for Mozilla. Once developing organizations get their new applications under a trusted framework, the next hurdle is maintaining a safeguard posture as those applications change over time and move into the cloud. Already struggling to ensure that their web applications are protected, the majority of security and compliance professionals believe the current trend of deploying to the cloud invites further vulnerabilities, according to a 2011 survey of 1,000 security and compliance professionals conducted by the Ponemon Institute and encryption vendor Vormetric. In the survey, less than 40 percent of respondents trust their own technologies to secure their sensitive data in the cloud – and less than one-third encrypt their sensitive data in the cloud.

Further, encryption is a cornerstone design point that should be considered in applications with sensitive data, yet it is one of the most difficult processes to achieve in the cloud, say experts. What other elements are needed in a secure design plan? It depends on who you ask, which vertical industry they are in, which type of cloud or web services they’re designing, and so much more, say Manico and Coates at OWASP.

However, there are several common design areas to focus on that apply to both web and cloud applications. This includes gathering business requirements; development and testing; access, authentication and data protection; configuration and zoning; visibility; and maintenance and continuity.

Development
Applications are written and upgraded by different coders at different times, and usually with no planning, say experts. They contain a patchwork of code, objects and platforms with known vulnerabilities, such as might be found in HTML5, Java, PHP, Ruby on Rails, JavaScript, and more.

With these applications going virtual into the cloud and even mobile, secure design must include ways to test the app before it’s even developed, then during and after development, says Gary Phillips, board member for nonprofit SAFECode, and senior director of technology assurance research at Symantec.

SAFECode, which stands for Software Assurance Forum for Excellence in Code, is supported by other large developers (including Microsoft, Adobe, SAP, Juniper Networks and Nokia) to advance best practices for more reliable software, hardware and services.

According to Phillips, secure code development practices are on the rise among commercial vendors. And, this is substantiated by a decrease in web application vulnerabilities, according to the latest “IBM X-Force 2011 Mid-year Trend and Risk Report.” For the first time in six years, the number of web application vulnerabilities declined, from 49 to 37 percent, among all vulnerabilities reported in the first half of 2011 compared to the same period the previous year.

On the other hand, the number of vulnerabilities listed as “critical” tripled, while the report authors expect mobile exploits to double in 2012. SQL injections and XSS vulnerabilities, input validation errors and numerous traditional attack methodologies are still prevalent in web applications, says Jack Danahy, director of advanced security at IBM. These, he says, must not be migrated into the cloud.

“We and cloud as platforms are both realizations of the distributed application,” he says. “I touch an application from somewhere offsite, gather a certain body of information, then touch something else and access other data.”

To determine which weaknesses attackers would attempt to exploit before an application is even developed, the application must be looked at from the point of its components, as a whole, and via its interactions with other applications. This is commonly referred to as the attack surface, says Dan Cornell, CTO of Denim Group, an application/portal development consultancy that also provides resources and training in this area.

Tools, libraries and APIs provided by OWASP SAFECode, the Cloud Security Alliance and others can help developers model threats to their applications, and discover where code, calls, interactions and functional aspects of the application could be made to fail.

According to Phillips, secure code development practices are on the rise among commercial vendors. And, this is substantiated by a decrease in web application vulnerabilities.

How are these apps, systems and clouds configured?

“Start by determining the value of the data that the application will contain or access. Cornell says. For example, if it involves personally identifiable information (PII) or financial data, the application will be a target. Next, model threats against that data by looking at the individual components of the application and its communication channels to pre-identify potential vulnerabilities at design time.”

“It’s much easier, cheaper and faster to repair vulnerabilities found during design rather than at implementation,” Cornell says. “But, quite honestly, a lot of organizations talk to us about being far ahead of old legacy applications that they can’t change, and are concerned about connecting them to other cloud and web-based applications.”

Cornell advises that organizations design secure workarounds – like connectors, APIs and hardening around the system. Or, if possible, use the new application design as a chance to upgrade old, insecure systems with new systems that can scale securely to web production, mobile access and cloud environments.

Configuration
“It’s critical to think about the type of applications customers run on the web and in the cloud as an extension of their intranet, collaboration system, or a retailer’s entire e-commerce site,” adds Omar Khawaja, director of security solutions for Terremark. Verizon’s cloud services subsidiary. “How are these applications, systems and clouds configured? And, more importantly, how are they securely accessed?”

As an example, Khawaja points to a customer-facing web application that processes financial transactions. During

Starting a secure design framework today will markedly improve the migration of applications to the cloud, reports Deb Radcliff.
Application design

the design phase, trust boundaries must be established between the web and transaction servers to protect the data. This seems like an obvious design point, but in virtual and cloud environments, these trust zones are more overlooked than they should be, say experts.

Further, when designing to commercial cloud providers, consider how customers are segmented from one another in the cloud service, says Phillips from Symantec. Secure zones should be set so that no customer can see into other customers’ data.

“Ten years ago we wouldn’t have put data from the KGB and CIA on the same RAID (redundant array of independent disks) of a storage service provider,” he says. “Today, cloud vendors need to deal with that same security challenge when hosting applications belonging to competing organizations in the same shared hardware and virtual infrastructure.” Users, he adds, need to work this out at the design stage and support separation rules with service-level agreements.

Identity federation, along with authentication and access standards – like OAuth (Open Authorization), XACML (eXtensible Access Control Markup Language), SCIM (Smart Common Input Method) and SAML (Security Assertion Markup Language) – are being designed today to meet access and security needs, according to Eric Olden, CEO of Symplified, an identity and access management vendor. “Access control, authentication, audit and administration all apply to cloud and web applications,” he says.

Encryption of sensitive data should also be tied to authorization, say industry experts. However, according to a survey by the Cloud Security Alliance, encryption offerings in the cloud are not as robust as they should be. The report recommends several layers of encryption for data in transit and in storage, in addition to key management.

“Any design plan must take the posture that the system will be breached and that the data inside will be accessed,” says Mark Bower, VP of product management at Voltage Security. “This is particularly true for payment transactions, which are essentially cloud-based services to merchants.”

He says the use of authentication should be tied to data encryption to limit exposure of the full live data – especially with new techniques, like format-preserving encryption.

“Encryption should also be used to protect live data from unauthorized users,” Bower says. “For example, to verify a transaction or to match a customer to an account, an operator may only need to see the last four digits of a Social Security number, or the last section of a credit card number versus the complete field.”

By now, most organizations should be encryptioning their sensitive information in a data-centric manner, which means sensitive material stays encrypted at rest, in transit and in use. If organizations are migrating to an infrastructure as a service (IaaS) where they’re responsible for their applications, it may suffice to replicate the same technique in the cloud through standards-based application programming interface (API).

If purchasing software as a service (SaaS), organizations should discover how the provider will help them carry their encryption and key management over into the cloud. For example, Volt age manages keys in the cloud for Volt age Cloud Service-based file and email encryption customers. Alternatively, enterprises may want to control their keys themselves with on-premise key servers for their apps in the cloud.

When considering application deployment to the cloud, the specific type of hosting environment will determine how security capabilities, such as encryption and monitoring, will be supported, says OWASP’s Manico. For example, in the IaaS model, the organization acquiring the service is responsible for its own applications. With SaaS, the provider manages the applications for the consuming organization.

Visibility and maintenance

Fuzzing, static analysis and functional testing are also critical during key stages of development, as well as after the application has been placed into production. So, design must include stages for testing the application, development and post-production.

Design also must include basic monitoring support, such as producing usable logs and registering changes to data and access, says Symantec’s Phillips.

There are numerous tools and services to test web applications for SQL injections, XSS and other code-based and functional vulnerabilities. However, when it comes to visibility into applications in the public cloud, organizations must rely on tools supported by their cloud provider to monitor their own data, say experts. To keep an eye on their provider’s network, they will need to rely primarily on contracts and annual audits.

Getting to a level of “secure by design” will take planning, time and coordination among business, development and security units, many say. But the task is not impossible.

“No one says secure by design is a quick architecture change that makes an application ready for the web or the cloud,” IBM’s Danahy says. “If it were easy, there would already be a common secure design template that everyone can use.”

—Gary Phillips, senior director, Symantec

To build trust, monitoring is very important...

—Peter Stephenson, technology editor

How we test and score the products

Our testing team includes SC Magazine Labs staff, as well as external experts with experience and expertise. In our Group Tests, we look at several products around a common theme based on a predetermined set of SC Labs standards (Performance, Ease of use, Features, Documentation, Support, and Value for money). There are roughly 50 individual criteria in the general test process. These criteria were developed by the lab in cooperation with the Center for National and Regional Security at Eastern Michigan University.

We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 15489) as a basis for the test plan. Group Test reviews focus on operational characteristics and are considered at evaluation assurance level (EAL) 1 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria-speak.

Our final conclusions and ratings are subject to the judgment and interpretation of the tester and are validated by the technology editor.

All reviews are set for consistency, correctness and completeness by the technology editor prior to being submitted for publication. Prices quoted are in American dollars.

What the stars mean

Our star ratings, which may include fractions, indicate how well the product has performed against our test criteria.

★★★★★ Outstanding. An “A” on the product’s report card.
★★★★ Carries out all basic functions very well. A “B” on the product’s report card.
★★★ Carries out basic functions to a satisfactory level. A “C” on the product’s report card.
★★ Fail to complete certain basic functions. A “D” on the product’s report card.

The big news this month is the addition of a new element: a set of reviews on emerging products that you can find exclusively on our website. Ready, this is more than emerging products. It’s more of an emerging market segments group. For example, this month we are addressing virtualization and the cloud. This is, truly, an emerging area of concern for security professionals. The virtual world is growing way faster than our ability to secure it. And there is a lot of confusion around the differences in clouds and virtualized systems.

For all of that, there are a few companies that have stepped up and addressed the issue. They have done it with imagination, ingenuity and market and technology savvy. We started dipping our collective toes into those murky waters a couple of years ago. We identified one of the few companies in this market space at the time, cited them as innovators for three years, promoted them to the Hall of Fame, and then they were mopped up by the king of virtualization.

Even with this new area of focus, we have not forgotten the meat and potatoes of the technology section: Group Tests. And we have a corer for you this month. UTMs have become a staple of our business, and the market is beginning to stabilize and mature. One of our favorite SIEMs, for example, was acquired recently by one of the security giants.

We have a bumper crop this month – 14 products, all of which are first-rate and hard to discern from one another. No worries, though, the two Miles (Stephenson and Lipinski) are shepherding these through theirpaces in the lab. They have the challenge well in hand. With our new full-page format, we are betting you will find a lot to think about this month.

And, as always, we’ll have a few thoughts at the start of the group, not to mention my thoughts – occasionally irreverent – on the topic of the cloud and its attendant hype. I am the sworn enemy of hype in our business, but you’ll probably figure that our fairly quickly.

So, it’s on with the show. To summarize, we have five emergents in the cloud and virtualization space (posted exclusively on the website), plus our Group Test of UTMs. That’s a lot to absorb in one month. So we’ll best get to it. Remember, we are always interested in your comments. Email me at pstephens@norwich.edu. I look forward to hearing from you.

—Peter Stephenson, technology editor

Adtran
A small device that provides full UTM P34

Kerio
Software that provides gateway firewall P40
Unified threat management (UTM)

This year’s crop of UTM tools are more of the same, only better, says Peter Stephenson.

**PICK OF THE LITTER**

For its smorgasbord of features and its ease of use, we make eSoft InstaGate 604 our Best Buy this month.

The gateProtect GPZ 2500 is at the higher end of the pricing spectrum, but has absolutely everything you would want in a UTM, making it well worth the price. Add the ease of setting up and managing it and we make it our Recommended product.

This month we explore unified threat management, or UTMs. The notion of UTM came out of the idea of multipurpose appliances back in the day. Today’s UTM is a sophisticated, multipurpose tool that can sit as a gateway and provide everything. This group has begun to mature and it is interesting to see the direction these tools have taken.

First, when we refer to a maturing group, we are talking about that point in its lifecycle where very little major innovation is occurring beyond that needed to keep pace with the genre. That certainly is the case here. While UTMs as a product group definitely are maturing, that does not mean that there aren’t some good products. We saw a strong showing this year. More of the same does not necessarily mean that the product type has become a yawn. Far from it in this case.

The UTMs we saw this year are beginning to stabilize into a coherent product type with a lot of similarities in the modules they provide. For example, we used to try to define a UTM based on what it could do. Did it have anti-malware? Did it have a firewall? If something was missing, we didn’t include it in the UTM review group.

Today, we don’t really have that problem. Most of the products we tested do anti-malware, firewall, some sort of content filtering, IDS (intrusion detection system)/IPS (intrusion protection system), and, perhaps, anti-spam. There are a few outliers that add additional functionality, but this pretty much defines the product type. These functions, though, are not trivial to deploy, especially in a single device that acts as an inline gateway. That is pretty much a recipe for a bottleneck. So there still are challenges.

A big one is malware. This is an emerging area of concern, still. It is emerging because it is always changing. We used to worry about zero-day threats. Now it can be zero-hour. Malware is proliferating at a ferocious rate. Add phishing that lets the bugs get inside the network without having to brute-force their way past a firewall and you have a real problem – and one that is growing in complexity daily.

A good UTM won’t let the bugs in, even when a user does something stupid, such as clicking on that attachment that we have told them a hundred times not to click on. So there is today’s UTM challenge: finetuning and keeping pace with the threats that are emerging and morphing on, at best, a daily basis. And that is no small task.

What we most wanted to know was how complete the new crop of devices is, how easy it is to configure a beast that does just about everything to protect the enterprise, and how effectively it protects that network without being a bottleneck to traffic.

There are months where the products in our groups are so close in functionality and capability that it is very hard to differentiate. There are months where that is not such a big problem. This group was, hands-down, the former. Differentiating among a bunch of mature, capable, full-featured products always is a struggle. This month, it was a big struggle. Two different reviewers put these products through their paces. They worked in separate locations, splitting the load between them, and still the products came up very close. That is another sign of a maturing market space.

Is it time for a new definition of UTM just to spice up the market? Probably not. What is more likely is that smaller, highly competent products will get sucked up by the big UTM companies or companies that make compatible products and need to round out their product lines. That’s the way it is in a maturing market, and we are ambivalent about its benefits.

No matter what, though, here is a solid, competent group of products that play a critical role in protecting your enterprise. There is a lot to absorb here so, with the caveat that next year might look quite different after the merger and acquisition machine kicks into gear, forge ahead and enjoy this month’s reviews. We certainly enjoyed producing them for you.

Mike Stephenson and Mike Lupino contributed to this Group Test.

### Specifications for UTM tools

<table>
<thead>
<tr>
<th>Product</th>
<th>Firewall</th>
<th>Intrusion prevention</th>
<th>Gateway anti-virus</th>
<th>Gateway anti-spam</th>
<th>Web content filtering</th>
<th>Application control</th>
<th>Built-in Wi-Fi</th>
<th>Active Directory integration</th>
<th>Predefined policy templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADTRAN NetVanta 2630W</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Astara Security Gateway v8.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elitecore Technologies Cyberasm CR1000vxa v10.01.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eSoft INSTAGATE 604 v5.0.20110603</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fortinet FortiWiFi-40C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gateProtect GPZ 2500 v9.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kerio Control v7.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M68 Security Secure Web</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSG Secure Web Gateway v3.01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netgear ProSecure UTM95 v2.0.16-0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smoothwall UTM-1000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SonicWALL NSA 4500 v5.8.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vasco Data Security xSguard Gateway-keeper v7.6.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WatchGuard Technologies XTM BSD Security Bundle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wedge Networks BeSecure 3005G AntiMalware Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ADTRAN NetVanta 2630W

The NetVanta from ADTRAN offers some nice functionality in a small package. This little device provides full unified threat management functionality for small to medium branch offices, and features include gateway-based anti-virus, firewall, SSL, and IPsec VPN, web content filtering and application control. This product also features a similar packet inspection engine that is found on SonicWALL appliances which works at the application layer to scan all files in real time to block possible hidden threats before they can enter the enterprise environment. Additionally, this product also includes built-in Wi-Fi to ensure protection of wirelessly connected devices.

The process for setting up and configuring the appliance is straightforward with the initial configuration being driven by an easy-to-follow configuration wizard. When the appliance is connected to the network, the wizard can be accessed from a web browser and takes just a few minutes to complete. At the completion of the wizard, the appliance network settings are configured and the rest of the configuration is done using the intuitive web-based management interface. The interface itself is organized very much like a SonicWALL interface as the NetVanta is driven by SonicWALL software. While we found the interface to be reasonably simple to get around, we did find ourselves having to click around a bit to get a good feel for where to find various settings.

As for policy configuration, this product offers a lot in terms of flexibility. The firewall comes with a few base policies already configured. These rules can be changed, or custom rules can be easily created to meet the needs of the environment. Firewall rules also can be configured to include web and application filtering rules, as well as intrusion prevention rules. These can be configured separately and then added onto the firewall rule with a simple click.

Documentation provided with this product only included a getting-started guide. This provides all the steps necessary to get the product connected to the network with a base configuration. We find this document to provide clear step-by-step instructions along with many screen shots, diagrams and configuration examples. While this guide provides a good overview of the product features, we find it to be a little too basic as a primary piece of documentation. We were unable to find any other pieces of documentation for the appliance, as well as quite a few screen shots and configuration examples in an organized, in-depth look at configuration and deployment of the product and product features. We find both pieces of documentation to include clear instructions, as well as quite a few screen shots and configuration examples in an organized, easy-to-read format.

ADTRAN offers the first year of software and hardware support as part of the initial purchase price of the product. After the first year, customers can purchase additional support as part of an ongoing support contract. Customers with support contracts can get access to phone- and email-based technical support along with product updates and firmware upgrades. Customers also have access to various hardware maintenance and installation services through the ADTRAN Custom Extended Service program. Some of these offerings include on-site and remote installation services and next-business-day equipment replacement.

At a price of $1,255 for the hardware and the first year of protection services, we find this product to be a solid value for the money. The NetVanta provides a lot of flexible configuration options, along with many protection options at a reasonable price.

Astaro Security Gateway

The Astaro Security Gateway is a flexible, full gateway security appliance that can be deployed and configured to fit almost any environment. This product is available as a full hardware appliance, software installation or virtual appliance. The Security Gateway offers firewall and intrusion prevention protection along with application control, web content filtering, gateway anti-virus, email content filtering and anti-spam.

We found deployment to be fairly easy with help from an initial setup wizard. The wizard is launched from a web browser once the appliance is connected to the network. This utility will help in creating the initial network settings of the appliance, as well as establish a base configuration of the security policy. At the completion of the wizard, all further administration and management is done via the web-based interface of the appliance. We found this to be well-organized and intuitive to navigate.

Policy and rules are also easy to create and manage. The base configuration that is put in place from the setup wizard provides a solid starting point for configuration of security policy, and many features can be easily customized by simply clicking them on or off. The appliance also comes pre-loaded with many intrusion prevention signatures – with most already enabled when the intrusion prevention system is turned on. Custom policy can easily be configured by using the base configuration as a template, which can be tweaked to meet the needs of the environment. The Security Gateway also incorporates Astaro’s branch security management toolset that allows for multiple appliances to connect together and be managed by a central device for a consistent blanket policy from one office to another. Furthermore, this product also can integrate with Astaro wireless security access points to provide protection to wireless devices.

Documentation provided with this product includes a short, one-page quick-start guide along with an administrator guide. The quick-start guide includes a few short instructions on how to connect the appliance to the network and get access to the web-based setup wizard. The administrator guide provides a more in-depth look at configuration and deployment of the product and product features. We find both pieces of documentation to include clear instructions, as well as quite a few screen shots and configuration examples in an organized, easy-to-read format.

Astaro offers phone- and email-based technical support to customers who have purchased a support and maintenance plan. Support is offered to customers at both 12/5 or 24/7 levels. Customers also receive no-cost access to a large web-based support area that includes documentation downloads, technical documents and a user forum. Astaro is also rolling out a brand new knowledge base that includes no-cost access to manuals and other documents.

A price of about $3,135 for the hardware, licenses for one year of network, web, mail, web application and wireless security subscriptions with premium 24/7 support, we find this product to be an excellent value for the money. The Astaro Security Gateway combines flexible deployment options with many gateway-based network security features that are easy to configure and manage in one appliance.

34 SC • March 2012 • www.scmagazine.com
Cyberoam CR1000ia

The Cyberoam CR1000ia is a full-feature network security gateway that provides solid protection from a multitude of threats. This appliance includes features such as a firewall, intrusion prevention system, gateway-based anti-virus, anti-spam, SSL, VPN and web content filtering, along with application control and flexible configuration options.

Installation and deployment of this solution is simple and takes only a few minutes to get a running base configuration in place. The initial setup is done by connecting the appliance to the network and accessing the web-based setup wizard. The appliance can be configured to run in bridge mode as a primary gateway or transparent mode to run behind an already existing router. The setup wizard is easy to follow. When complete, a base configuration is put in place that could run well with out much need for tweaking. However, this appliance is highly customizable and can be configured to meet the needs of any environment.

Aside from the base policy, this tool features many configurable controls, including a plethora of application control options. These application controls also include instant messaging (IM) controls, which allow for logging and customized security control over public IMs for communication modes, including chat, file transfer and audio-video. As well, the appliance comes pre-loaded with quite a few security templates, including web security and a solid general-use policy, which can be customized. The only problem we had with the configuration was we found it to be less intuitive in certain areas, requiring us to click around a bit to learn how to create custom policies and rules.

Documentation includes a short quick-start guide along with a PDF user guide and several other supplemental documents. The quick-start guide provides the steps necessary to get the product up and running, while the user guide focuses on in-depth configuration and use of the product features. Cyberoam includes technical support as part of the ongoing subscription cost of the appliance features. Customers can choose from many subscription options, including ongoing updates, phone and email technical assistance, hardware warranty and replacement services. In addition to phone- and email-based technical support, Cyberoam also offers online chat-based technical support. As well, customers can access no-cost support resources via the support area on the website. This area includes a knowledge base, FAQ section and other resources.

At a price just shy of $19,500 for the fully loaded appliance with subscriptions to anti-malware, anti-spam, web and application filter and intrusion prevention system, eight-hours-a-day/five-days-a-week support, hardware warranty and return merchandise authorization (RMA) fulfillment for one year, we find this product to be a good value for the money. The Cyberoam CR1000ia includes a lot of built-in functionality for solid gateway security at a reasonable price. Customers also can purchase specific modules à la carte to further customize cost and appliance options. – MS

eSoft InstaGate 604

Back again is one of our favorites from eSoft. The eSoft InstaGate provides solid protection designed for the small to mid-sized business environment. This appliance features integrated services – such as a full stateful inspection firewall, intrusion prevention system, web content filter, anti-virus, anti-spam and email content filtering – all under one easy-to-manage platform.

The first thing to note with this appliance is the ease with which it can be set up and configured. When the appliance is plugged into the network the first time, it can receive a dynamic host configuration protocol (DHCP)-assigned address for initial configuration or one can be easily statically assigned to it. Once it has an address, the setup is all done via a web-based wizard. This is easy to follow and includes steps to not only configure network settings and get a base configuration, but it also runs connectivity diagnostics and downloads updates if necessary. This way, at the completion of the wizard the administrator can be assured that the appliance is connected to the network properly and it is updated and ready to go.

After the setup wizard is complete, all further management is done via the web-based management interface. We found this to be easy and intuitive to navigate. We also found that many of the configurable policy options were as simple as turning them on or off. The InstaGate also does an excellent job of visual reporting in real-time. The main dashboard, also known as the Threat-Monitor, provides many easy-to-read graphs and charts that show real-time alert and traffic data for a nicely detailed overview of network security. The InstaGate also incorporates the use of ThreatPaks from eSoft. These come in two flavors: The Web ThreatPak includes features for web security, intrusion prevention system, and gateway anti-virus and anti-spyware. The Email ThreatPak includes all the functions of the Web ThreatPak, but also adds functionality for email functions, including a spam filter and built-in email server.

Documentation includes a quick-start guide and a PDF user guide. The quick-start guide details the initial setup procedure for getting the appliance up and running in the environment, including a step-by-step walkthrough of the setup wizard. The user guide provides a much more in-depth look at configuration and management of the product features.

The company offers 90 days of no-cost, technical phone support as part of the purchase price of the appliance. Customers can purchase additional help on an as-needed basis or as a part of a support bundle. Support bundles include access to phone- and email-based support, software support, and hardware support. Customers also receive no-cost access to an online area, which includes documentation downloads and a knowledge base.

At a base price of about $2,000, plus around $1,500 per year for ThreatPak subscriptions, we find this product to be an excellent value for the money. The eSoft InstaGate provides many easy-to-configure features, along with easy deployment options to provide solid network protection at the gateway. – MS
Fortinet FortiWiFi-40c

This little device proves that one does not have to have a gigantic piece of hardware taking up a ton of rack space to have solid perimeter security. The FortiWiFi-40c from Fortinet provides features such as a firewall, intrusion prevention system, application control, virtual private network (VPN) and web content filtering all in one device. This product is built on the same FortiOS platform that its much larger counterparts use, so this device houses powerful inspection and security engines that rival the much bigger systems. The FortiWiFi also incorporates Wi-Fi security function to ensure wireless devices receive the same protection against threats as the wired ones.

From box to management, this tool is relatively simple to use. The initial configuration is quite easy and, following a simple setup wizard, takes just a few minutes. The wizard aids in setting the network configuration, as well as the base security policy. At the completion of the wizard, all further management is done via the web-based management console. We found this console to look exactly like the Fortinet consoles we have used in the past, but it is boiled down to fit the appliance of the application. There were some areas in which we struggled a little with configuration in this simplified version of the interface.

We found policy management to be slightly more difficult to administer as most of the policy had to be built from the ground up. While this does provide for a lot of customization, it also allows for possible human error, which can lead to a lot of troubleshooting. We would like to see a more comprehensive base policy from which to build versus having to start at the beginning on our own. With that said, we did have an overall good experience with the interface after some tinkering and experimenting with settings.

Documentation provided with this product included a short quick-start guide, which outlined the appliance itself and how to complete the initial configuration steps. Other documentation was included on a supplemental CD, and was comprised of several manuals and guides for configuring and managing the appliance and all of its features. This material also included a full administrator guide with a lot of configuration steps and examples, along with a good number of screenshots organized in an easy-to-follow format.

Fortinet includes the first 90 days of 8/5 technical support as part of the purchase price of the product. At the end of the 90 days, customers can purchase additional assistance as part of an ongoing support subscription. This support includes both 8/5 and 24/7 phone and email technical support tiers. The plans also include access to product updates and upgrades, and subscriptions to the various security services for the appliance. As well, customers can access a large support area via the website, which includes product documentation downloads, technical resources and a knowledge base.

At a price just under $450 before support and subscription costs, we find this product to be a good value for the money for smaller environments that may not require the larger more expensive offerings. This gateway provides a solid feature set that can be configured and customized to meet the needs of almost any type of smaller environment. – MS

gateProtect GPZ 2500

The gateProtect GPZ 2500 is quite possibly the be all and end all of perimeter network security. This appliance features the standard UTM functionalities of firewall, intrusion prevention system, anti-virus, anti-spyware, web content filtering and email content filtering, but the features do not stop there. It also features application management, single sign-on capabilities, zero hour mail protection, as well as load balancing and virtual local area network (VLAN) capabilities, to name a few. Using this appliance at the gateway can enable administrators to easily manage strong network security policy without sacrificing speed or performance.

The big piece of this product is its flexibility and configurability. A couple of years ago when we first reviewed it, we had trouble making it work properly. We thought it was awkward and difficult to use. However, last year we spent some time learning how to use it and found it to be a lot easier to configure than we originally thought. Well, this year we did some more experimenting and found that no matter the complexity of the environment, this product can be configured to provide granular control and security policy without being overly complicated.

The initial configuration of the appliance and all management is done using a client application-based management console. The console itself can be a little overwhelming at first, but after some clicking around becomes quite comfortable and familiar. This solution takes a different angle on policy configuration. It uses what will essentially become a network and group map to assign policy. All configuration involves simply a drag-and-drop of components, such as user or network groups, onto the desktop of the management interface and then connecting them. The connections can then have policy attached and the product is configured. At the completion of configuration, the desktop will provide an easy-to-view map of how and where policy is applied, so adjustments or additions can be easily made without having to go through lines and lines of rules.

Documentation includes a one-page quick-start guide, along with a PDF user manual. The quick-start guide provides a few short steps that are necessary to get the appliance connected to the network, as well as access instructions for the management interface. We found all documentation to be well-organized and easy to follow.

Customers who purchase gateProtect appliances receive 24/7 phone and email technical support at no cost for the first 30 days after purchase. After 30 days, customers can purchase additional assistance through an annual plan which is available in two levels. These include 24/7 phone- and email-based technical support.

At a price just shy of $16,500, this solution may seem quite pricey at first. However, we find the gateProtect GPZ an excellent value for the money. It combines a high amount of functionality and flexibility with an easy-to-use management interface that can streamline perimeter and network security policy with minimal effort from administrators. – MS
Kerio Control from Kerio Technologies is an interesting product in this space. This tool is comprised of software that can be installed on a dual-booted Microsoft Windows machine at the gateway or it is available as a virtual appliance for use in a VMware ESX environment. Once installed, this product can provide gateway firewall and intrusion prevention, along with spam, spyware and virus protection, web content filtering and email virus protection. Kerio Control also provides VPN capabilities and network monitoring and bandwidth control.

We found this tool to be easy to use from installation through configuration and management. The installation itself consists of running an executable that launches an installer package. After a short setup wizard, the installer implements all the components, including the web-based management console. At the completion of the install, all further configuration and management is done using this utility. We found the console itself to be easy to navigate with a clean and organized look.

Policy configuration is also quite simple, and policy can be configured to be broad or quite granular based on users or groups. Initial connectivity is easily set up using the network rules wizard. At the completion of this step, the base set of network access rules for the firewall are put in place, and configuration of the other services, such as the web filter, can be started.

We found that the majority of the initial configuration was straightforward, but did require some time clicking around and setting up policy. However, we liked the available integration with the already existing Active Directory user and group infrastructure for managing group and user policy. This product also can integrate with an external anti-virus engine, along with the built-in AV engine, to provide an extra layer of virus scanning to the environment.

Documentation includes a step-by-step guide that details initial deployment scenarios with many useful diagrams, along with a full administrator guide. The administrator guide covers the product from installation through advanced configuration of the product features. We find this guide to be well-organized with many step-by-step instruction and quite a few screen shots. We would like to see more screen shots and configuration examples for the initial configuration process, but for the most part we find the document to be easy to follow.

Kerio offers full 24/5 phone and email technical support to all customers with an active license. Customers also have access to a small help area on the website, which includes product documentation downloads and a knowledge base.

At a base price of $265 for the first five users, and $26 per user after that plus the cost of hardware, we find this product to be an average value for the money. While it may be a reasonable offering for smaller environments, this solution is not very cost-effective for larger environments. We find that while it did have some decent functionality, it does not provide much in the way of robustness. This paired with an annual renewal cost starting at around $8.70 per user per year, and we find this product to have an overall high cost of ownership. – MJ

M86 Secure Web Gateway v10.1

M86 Secure Web Gateway (SWG) proactively safeguards against malware and Web 2.0 threats using patented real-time code analysis (RTCA), dynamic web repair (DWR) technologies, and granular social media controls. The product is deployed as a policy server and scanning server. In a typical environment, one would deploy multiple scanning servers managed by a centralized policy server. For our review, we configured both on the single appliance.

The product is delivered either as a pre-loaded server-based appliance or as a virtual SWG appliance that works with a VMware ESXi v4.1 server. A physical 3000 series appliance was delivered to our lab. Initial setup does require some command line work as one needs to either secure shell (SSH) through the local area network (LAN) or terminal via the serial port. One needs to set up the appliance first (running a set up command) and then configure the network functions through the command line before being able to use the web-based user interface. One can configure the tool for explicit or transparent proxy, in-line bridge mode, proxy chaining, integration as an Internet content adaptation protocol (ICAP) service or as a client with web cache communication protocol (WCCP) v2. Once the network portion is configured, one can browse to the appliance IP and use the web-based user interface to perform the remaining configuration and management functions. The management console provides administrators with a tool for managing the entire Secure Web Gateway deployment from the policy server.

Website code or file content and behavior are analyzed in real time by identifying operations, parameters, script manipulations and other exploitations for a given piece of content. M86 can view in real time whether a piece of active content will perform a malicious action when loaded into a browser. In accordance with pre-defined security policies, M86’s security system dynamically decides if content is safe for browsing, providing real-time protection. M86’s granular social media control gives organizations the power to block posts, comments or uploads to social media sites. There is also support for web page repair, data leakage protection, application controls, SSL inspection and certificate error handling, and digital signature analysis of binary objects. As well, M66 code analysis includes handling of code splitting. There is full lightweight directory access protocol (LDAP) and Active Directory integration available for user authentication. There are a number of anti-virus and URL scanning options, each licensed separately, but one does have choices on scanning engines.

Basic eight-hours-a-day/five-days-a-week support is provided with the subscription fees. Gold and platinum support is available for 10 and 20 percent fees, respectively. Implementation and management documentation is not very comprehensive. We had to figure out a lot of the items on our own. The offering has a lot of enterprise-level capabilities, but it is limited to web content filtering and requires a lot of work to set up and configure. Load balancing is only integrated in the high-end chassis solution. – ML
NETGEAR ProSecure UTM9S v2.0.16-0

T
he NetGEAR UTM9S is an all-in-one security appliance that is deployed at the internet gateway. It features a stateful packet inspection firewall, intrusion prevention systems (IPS), SSL, VPN (secure sockets layer virtual private network), internet protocol security (IPsec) VPN, anti-malware, anti-spam, web URL filtering and application control. It also has some solid small/home office features, such as modular UTMs slots for wireless and DSL modules.

Setup was fairly straightforward. We connected the appliance to our test network, we connected to the internal port, set up the addressing for the internal local area network (LAN), set up the addressing for the external wide area network (WAN) and configured dynamic host configuration protocol (DHCP) for our test network. The user interface is nicely laid out and was easy to use. The menu options are contained in multiple bars across the top of the browser page and configuration options are tabbed in the window below. There is a setup wizard, but we chose to do our configurations manually. Within about 15 minutes, we configured our firewall, our email anti-virus settings, anti-spam, URL filtering, blacklist and scan exclusions. The appliance also supports full VPN, including SSL and IPsec. Although we did not configure or test the VPN options, we see that it supports NetGear’s ProSafe VPN Client, along with point-to-point tunneling protocol (PPTP) and Layer 2 tunneling protocol (L2TP) options. There is also a nice wizard for configuring either SSL or IPsec VPNs. Our appliance shipped with a DSL module and internal wireless bridge module. We did not test either of these options, but the configuration was made easy as it was all integrated within the same user interface. It was a nice feature to have options for the WAN and LAN connectivity, as well as the ability to use this for backup connectivity if needed.

The UTM9S combines a stateful packet inspection firewall with a content scan engine that uses NETGEAR stream scanning technology to protect the network from denial of service (DoS) attacks, unwanted traffic, traffic with objectionable content, spam, phishing and web-borne threats, such as spyware, viruses and other malware threats. Stream scanning is based on the observation that network traffic travels in streams. The UTM scan engine starts receiving and analyzing traffic as the stream enters the network. As soon as a number of bytes are available, scanning starts.

This product was extremely easy to set up and configure in our test environment. Within minutes, we had an operating solution. The documentation is complete and well done. The product comes complete with 24/7 support and advanced hardware replacement for the first year bound price, and is renewable for $35 a year thereafter. This product offers a lot of gateway protections at an attractive price point. The model we tested is rated at 130Mbps throughput on the firewall. Other models in the family can scale to 900Mbps. We would recommend doing some performance testing in large environments if you intend to use all of the appliance capabilities. – ML

<table>
<thead>
<tr>
<th>GROUP TEST</th>
<th>UTM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NETGEAR ProSecure UTM9S v2.0.16-0</strong></td>
<td><strong>SmoothWall UTM-1000</strong></td>
</tr>
<tr>
<td><strong>Vendor</strong></td>
<td><strong>Vendor</strong></td>
</tr>
<tr>
<td>NETGEAR ProSecure</td>
<td>SmoothWall</td>
</tr>
<tr>
<td><strong>Price</strong></td>
<td><strong>Price</strong></td>
</tr>
<tr>
<td>$536 (hardware plus one-year subscription bundle) plus $56 (Wireless-N module) plus $91 (DSL module)</td>
<td>MSP $15,500 for 500 computers/devices</td>
</tr>
<tr>
<td><strong>Features</strong></td>
<td><strong>Features</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ease of use</strong></td>
<td><strong>Ease of use</strong></td>
</tr>
<tr>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td><strong>Performance</strong></td>
</tr>
<tr>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Documentation</strong></td>
<td><strong>Documentation</strong></td>
</tr>
<tr>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td><strong>Support</strong></td>
</tr>
<tr>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Value for money</strong></td>
<td>★★★★★</td>
</tr>
<tr>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>OVERALL RATING</strong></td>
<td>☆★★★★</td>
</tr>
<tr>
<td><strong>Strengths</strong></td>
<td>Scalable and full-featured</td>
</tr>
<tr>
<td>Full-featured offering at an attractive price point.</td>
<td></td>
</tr>
<tr>
<td><strong>Weaknesses</strong></td>
<td></td>
</tr>
<tr>
<td>Centralized management is not yet available for multiple appliances. Although this is coming later in 2012.</td>
<td></td>
</tr>
<tr>
<td><strong>Verdict</strong></td>
<td>Makes a lot of capabilities and is easy to set up and use.</td>
</tr>
</tbody>
</table>

SmoothWall UTM-1000

T
he SmoothWall UTM-1000 appliance combines SmoothWall Guardian Web Security with the network security functions of firewall, intrusion prevention and detection system (IDS/IPS), internet access control, virtual private network (VPN), instant messaging control, load balancing, wide area network (WAN) aggregation, GFI VIPRE anti-malware, MailShEll email anti-spam/phishing and bandwidth management. The product was delivered to us as a hardware appliance and we saw in the documentation that there is an option for a software version if one is desired. The UTM-1000 model we tested was rated for a 500 to 700 user environment. There are options for smaller models supporting 50 and 100 user environments.

Setup begins with browsing to the default IP and port and using the web-based interface to do initial network setup and subsequent configuration and management. Setting up the appliance on a network requires a simple addressing of the internal interface and then setting up the proper internet service provider (ISP)/internet properties. Once on the internet, we verified our licensing and ran an update. The user interface (UI) was somewhat clunky at first, but after using it for a few minutes and realizing that the intent of the design is really geared to keeping one just a few clicks away from any options, it became a bit more intuitive to use.

SmoothWall-UTM provides web security by providing a web security policy. A web security policy, containing filters and, optionally, time settings and authentication requirements, determines how SmoothWall handles web content. The firewall did deliver stateful inspection, including layer 7 content analysis. However, the firewall programming was not as user friendly as we would have liked. In fact, it is more like mapping port forwarding rules. There is pop-up help available on various screens for some configuration assistance, and there are a lot of templates available in the various sections for use. There is also a default web security policy in place that one could use to get the product up and running quickly.

The product features are very complete, with full virtual private network (VPN) support for both secure socket layer (SSL) and internet protocol security (IPsec). Web filtering and control features include dynamic filtering of page content, context and construction and URLs, “who, what, when,” granular policy tools, mobile device filtering for iOS, OSX, Windows, Android and bring your-own-device (BYOD)/guest filtering.

There was a good selection of base reports available with export capabilities to .csv, Excel or PDF formats. There is alerting built in as well. However, from what we are able to see, it appears that these alerting capabilities are pre-programmed and we do not see an ability to add to those. Basic support only includes phone and email assistance for 30 days.

The SmoothWall UTM-1000 is feature rich and has all the necessary enterprise features to handle the needs of any medium to large organization. However, the pricing is a bit on the high side at approximately $15,000 for 500 computers/devices. – ML

<table>
<thead>
<tr>
<th>DETAILS Vendor</th>
<th>UTM-1000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor</strong></td>
<td>SmoothWall</td>
</tr>
<tr>
<td><strong>Price</strong></td>
<td>MSP $15,500 for 500 computers/devices</td>
</tr>
<tr>
<td><strong>Features</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Ease of use</strong></td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Documentation</strong></td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Value for money</strong></td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>OVERALL RATING</strong></td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Strengths</strong></td>
<td>Scalable and full-featured</td>
</tr>
<tr>
<td><strong>Weaknesses</strong></td>
<td>Not many: configuration can be a bit complex, price.</td>
</tr>
<tr>
<td><strong>Verdict</strong></td>
<td>Features and performance make this a strong consideration for an enterprise solution.</td>
</tr>
</tbody>
</table>
SonicWALL NSA 4500 v5.8.1

The NSA 4500 is a purpose-built appliance that can be deployed at the edge of a network, inside a network between various network segments, or inline behind existing security solutions. It is managed through a graphical user interface or a central management console, called Global Management System. We tested with the standard web-based user interface. The NSA 4500 appliance offers an extensive array of security and networking features and it is easy to deploy and manage in a wide variety of environments. As a suite of appliances, the NSA protects against a comprehensive array of attacks, combining intrusion prevention, anti-virus and anti-spyware, anti-spam and content filtering with application intelligence, control and visualization, with advanced routing, stateful high-availability and high-speed internet protocol security (IPsec), and secure sockets layer virtual private network (VPN) technology.

We attached the appliance to our internal test network and our internet switch. We pointed a browser to the default IP address of the appliance and configured the local area network (LAN) and wide area network (WAN) ports for our environment. Configuration was simple as the user interface (UI) is clean and intuitive. But, there is a separate step involved in setting up these appliances in that one must first set up a mySonicWALL account through the UI, and then point the appliance to that account for licensing and updates.

This is a full-featured product with support for stateful firewall, anti-virus and anti-spyware for both email and URL, application control, intrusion prevention systems (IPS), deep packet inspection for SSL, and VPN. There is also a packet capture and monitor available right in the UI. Configuring the firewall rules was quick and easy. There are default access rules that one can edit or individual rules can be added in.

There are enterprise features, such as high availability failover pairs and performance throughput on stateful inspection mode of 275Gbps. There is a useful GeoIP filter option for quickly and easily blocking IP ranges by region. There is also the ability to do SSL traffic stateful inspection (DPI-SSL). Voice over internet protocol (VoIP) traffic is supported through the appliance without the need for a separate session border controller.

The dashboard capabilities are very well done, with numerous dashboards to choose from with configuration options for displayed data. Most of the reporting is done through the dashboard function, including the built-in threat reports. Logging is fairly basic with some nice tools for mining the log data. Alerting is limited to setting an alert level on events, and this is delivered via email.

Documentation was not provided with the product when it arrived, but we were able to obtain it all from the mySonicWALL site. Support is available for 90 days with options to purchase either eight-hours-a-day/five-days-a-week or 24/7 a year add-on for 17 or 23 percent of list price, respectively. This is a very strong offering with the features it delivers for the price point. The ease of use and dashboard features make it easy to manage. – MI.

OVERALL RATING ★★★★★

Strengths Dashboards, packet capture tool, session initiation protocol support.
Weaknesses Nothing of real note, maybe a bit more capability in user interface.
Verdict A bit of functionality and performance for a decent price. Full featured, yet easy to use.

VASCO Data Security aXsGUARD Gatekeeper v7.6.4

The Vasco aXsGUARD Gatekeeper v7.6.4 is an authentication appliance intended for small and mid-sized enterprises.

In addition to strong authentication, the aXsGUARD Gatekeeper has the potential to manage more of an enterprise’s internet security needs. Its modular design means that additional software options can be purchased at any time, and specific features can be enabled or disabled as required, including content scanning for email and web access and virtual private network (VPN) management. Users can connect using strong authentication, or with a client, such as point-to-point tunneling protocol (PPTP), internet protocol security (IPsec), Layer 2 tunneling protocol (L2TP) or secure sockets layer (SSL), along with other connection options, such as web portal or reverse proxy.

The initial setup was done through connecting a PC via a crossover cable to the appliance. One has to first login and create a new administrative user and then log out and back in again with that new user. We then set up the local area network (LAN) and wide area network (WAN) ports to our test network specifications. Once we had the base configuration complete, we were able to browse to the appliance and log into the user interface for configuration and management activities. The user interface (UI) was not the easiest we have used, as we find a lot of the programming to be cumbersome. Additionally, we did not like the fact that simple changes required a reboot of the appliance. With the combination of the UI and the required reboots, it took us some time to get the system into a useful state. There were some examples available for setting up users and policies.

The product is geared to manage security from the authenticated users’ perspective. Everything is seen from the view of the end-user, so all surf and mail policies are preferred to be determined on a user base rather than machine (IP) base. Depending on user rights, admins can allow users to surf within time restrictions, blocking or allowing specific sites based on URL or content. For email, multiple defense systems – like blacklists, greylists, two anti-virus engines, anti-phishing and anti-spyware engines – are in place. Basic firewall and intrusion prevention system (IPS) features are provided along with the virtual private network (VPN) support, directory service integration (including RADIUS) for importing users and groups, and strong authentication through the built in VACMAN controller. We were also provided the option of content scanning that adds features, such as email anti-virus and anti-spa,m user-based role creation and web monitoring.

The documentation is complete and definitely helped us through the setup and configuration. Eight-hours-a-day/five-days-a-week support for the first year is included in the purchase price, with renewal options at $175 per year. Scanning licenses are $25 per year per user. 24/7, VIP support and pay per incident are all available options for purchase. The price point is very attractive and the authentication-driven approach is a good one. However, one will need some patience to get this device set up. – MI.
WatchGuard XTM 810 Security Bundle v11.5.1

The WatchGuard XTM 810 Security Bundle is a full-featured security appliance for midsize businesses. It combines signature and heuristics-based anti-malware, recurrent pattern detection anti-spam, and multi-layered anti-phishing (anti-virus, reputation, URL filtering and content-type filtering). XTM 810 controls more than 1,800 unique applications using a hybrid signature and behavior analysis engine. It includes a firewall, application control, anti-virus, intrusion prevention systems (IPS), web filtering, anti-spam and reputation-enabled defense for protection against multiple classes of threats. It also features site-to-site and remote access virtual private networks (VPNs), identity-based policy creation with support for Windows Active Directory and LDAP (lightweight directory access protocol), traffic shaping, multi-WAN (wide area network) support and virtual local area network (VLAN) support.

Initial setup was pretty simple. We plugged in the appliance to our internal switch and our internet switch. Our test systems were handed an address via dynamic host configuration protocol (DHCP) in the default IP range, and we were able to browse to the web-based user interface, set up the network configuration we desired, set up the internet interface, and we were ready to program the device. For the initial configuration of an XTM appliance, there is a quick-setup wizard accessible either via a browser or from the WatchGuard System Manager application. We used the web-based user interface (UI) for our testing. It is important to note that there is a system manager application that comes with the product for managing the device or multiple devices from a centralized location. One also has the ability to set up multiple configurations under this model and configure pop-up alerting. There is a policy manager tool for creating and modifying policies. The intrusion detection system (IDS) function works like any other intrusion prevention system (IPS), but in this case there is a nicely integrated common vulnerabilities and exposures (CVE) reference function to look up information on a particular signature from right within the interface. There are also IDS policy templates for one to customize. Anti-malware is provided using AVG’s signature match and behavioral analysis engines.

Logging can be kept on the appliance or sent off to a log host. Alerting is available and tunable by specific events and is delivered via email. Dashboarding is available for most system and security functions. Reporting is available with the application control features. Documentation for the tool is very well done. One year of LiveSecurity Plus is included with the XTM 810 Security Bundle, and support is sold on a three-incident pack basis for $519. From an investment protection standpoint, one is able to upgrade to the next higher model with the purchase of a software license key. The price as tested at $12,805 puts this in the middle to upper price range, but one gets a lot of functionality in an easy-to-use solution.~ML

Wedge Networks BeSecure 1005G Anti-malware Gateway v4.0.1

The BeSecure Anti-malware Gateway is a family of web security appliances, capable of real-time deep content inspection for thousands of concurrent web, email, and FTP sessions. BeSecure incorporates best-of-breed content security techniques to protect the network by inspecting commonly used application layer protocols, such as HTTP, SMTP, POP3, IMAP and FTP. We tested the 1005G model, which is sized for mid-sized organizations or 500 users. There is also a software option available for VMware virtual environments.

Initial configuration was done by connecting our test PC via a crossover cable to the ingress interface. Once we configured the network components, we were ready to move on. We did not have to license our appliance as that was already done for us. The flexible deployment options make this product easy to integrate into any environment. We chose a transparent bridge mode option for our testing, but one has various route-based modes, web cache communication protocol (WCCP) or internet content adaptation protocol (ICAP) options and high availability cluster mode options. The product focuses on content inspection, so configuration is focused on these features.

There really isn’t a firewall or intrusion detection system (IDS) component. One can map protocols to ports, but that is really all the configuration admins do at that level. That said, it does do content inspection and data leakage protection very well. Keyword filtering for data leakage and breach prevention allows content to be inspected down to individual words and patterns contained within web traffic. These features are fully customizable with specific expressions, enabling organizations to prevent the leakage of confidential information leaving the organization through internet protocols.

With an Open Service Bus (OSB) technology, BeSecure easily integrates with best-of-breed security engines, including complete Kaspersky malware signature database, heuristic ability and per-hour signature updates. It also contains a Cloudmark anti-spam, anti-phishing engine that is updated every 45 seconds. An add-on option contains a complete SmartFilter web filter database with 90 plus web categories, including malicious sites. There is an option for traffic capture, but it is limited to a 10MB file size and there isn’t a way (that we found) to review it on the appliance.

Logging is contained on the appliance and also can be configured to send off to a syslog server. Event monitoring and searching is easy to use. Alerting is available for certain security and system events, and is sent out via email. Reporting is a strong point and is well done. Dashboarding is excellent, with the ability to drop data to a report and export it to a .csv or PDF. Documentation is complete. The initial setup guides are sufficient to get up and running and the user manuals are built into the interface. Support must be purchased on top of the product purchase and there are basic, eight-hours-a-day/five-days-a-week and 24/7 options available.~ML
The always-on resource for IT professionals

As a complement to our annual SC Congress Conference and Expo events, SC Magazine has launched a permanent website environment that will be open to our readers around the clock all year long. Each month we host an event on the site focused around a pertinent subject that you as an IT security pro face on a regular basis. This is a completely FREE offering to keep you informed of the newest developments in the industry. Participants can earn up to eight CPE credits for an eConference & Expo, and two CPE credits for a Virtual Symposium.

Join us for our next virtual events

March 20-21 – PCI compliance:
This eConference will provide updated guidance on how you can assure your organization remains compliant and keep all-important personal identifiable information secure. Guest speakers explore this and more.

April 24 – Cyber espionage:
Hacktivist groups have made it clear that no computer network are immune from penetration. Perhaps today’s top challenge facing senior IT personnel is to get the C-suite to sign off on implementing a 24/7 security system before the enterprise suffers a breach.

For a complete schedule and to register, visit our 24/7 site: scmagazine.com/scwc247

Upcoming events

May 17
eSymposium:
Advanced monitoring and forensics
May 24
eSymposium:
Privacy and security
June 7
Canadian eSymposium
June 21
eConference: Auditing and compliance
July 12
eSymposium: Database security
July 24
eConference: Securing the cloud
Aug. 23
eSymposium: Social networking security
Sept. 6
eSymposium: Mobile security
Sept. 18
eConference: Data security
Oct. 9
eConference: PCI
Oct. 25
eSymposium:
Advanced persistent threats
Nov. 15
eSymposium:
Vulnerability management
Dec. 4
Canadian eSymposium

For more information

SALES
Mike Alessie
National accounts manager
(646) 638-6002
mike.alessie@haymarketmedia.com

EVENTS
Anthony Curry
Senior events coordinator
(646) 638-6009
anthony.curry@haymarketmedia.com
The time is now

Last year saw record-setting numbers of data compromises, which is expected to finally drive home the reality that to successfully defend against and react to today’s cyber attackers, robust information security practices must be supported and championed top-down and corporate-wide.

Too much at stake. We see hacktivist groups launch attacks on government and private entities.

Alongside these, more traditional cyber thieves pinch customer data to use or sell off to the highest bidder and foreign spies seek coveted intellectual property from high-profile companies. Further, organizations’ burgeoning data sets and their analysis and application are predicted to become major drivers for jumps in productivity, customer interaction and product/services innovation. “Big data” means big competition, and those companies that have a sound understanding of theirs are sure to win out.

But challenges in securing this central trove of assets abound. And communication and cloud computing applications. No doubt, a further spike in brand-damaging attacks is bound to happen.

Yet, information security is going mainstream, which means IT-savvy and not-so-IT-savvy consumers expect their private information to be safeguarded. Legislators do, as well, hence all the bills meeting through the halls of the U.S. Congress.

Luckily, this means all the information security professionals and technology providers we’re honoring tonight are getting more widely acknowledged as critical to the success and longevity of businesses. So, through our Reader Trust Awards, and more widely acknowledged as critical to the success and longevity of businesses. So, through our Reader Trust Awards, and more widely acknowledged as critical to the success and longevity of businesses.

We’re honored tonight to celebrate them all during our 2012 SC Awards for yet another year – one that is seeing cyber security practices becoming a common entity from the majority. – Illena Armstrong, VP, editorial director, SC Magazine

EASTERN REGION SALES MANAGER
Mel Sweeney (610) 838-6020
NATIONAL ACCOUNT MANAGER - EVENT SALES
Mike Denton (610) 838-6022
ACCOUNT EXECUTIVE
Deena Kost (610) 838-6022

EDITORIAL
VP, EDITORIAL DIRECTOR
Mary Altman
EXECUTIVE EDITOR
Don Kaplan
MANAGING EDITOR
Greg Masters

2012 SC AWARDS U.S.
EVENTS DIRECTOR
Nikharshala Nallu
SENIOR EVENTS COORDINATOR
Anthony Cury
SC Magazine would like to thank all of our sponsors for their generous support of the 2012 SC Awards U.S. Their involvement has made this event possible, which helps raise professional standards in the information security industry worldwide.

Cisco
www.cisco.com/go/security
Cisco simplifies the task of addressing today’s security requirements, regardless of application or service.

HP Enterprise Security
www.hpenterprisecurity.com
HP is a leading provider of security and compliance solutions for enterprises that want to mitigate risk in their hybrid environments.

Qualys
www.qualys.com
Qualys solutions are deployed in hours anywhere, providing customers a continuous view of their security and compliance postures.

Schwartz MSL
www.schwartz-pr.com
Schwartz MSL, the technology innovation firm, drives strategic communications programs for some of the most successful security companies.

Splunk
www.splunk.com
Splunk software collects, indexes and harnesses the massive machine data generated by websites, applications, servers, networks and mobile device.

Teleperformance
www.teleperformance.com
Teleperformance develops and manages customer acquisition, customer care, technical support and debt collection programs around the world.

Tenable Network Security
www.tenable.com
Developed a unified security monitoring approach based on the Nessus scanner engine for securing enterprise networks worldwide.

F5 Networks
www.f5.com
F5 Networks helps the world’s largest enterprises realize the full value of virtualization, cloud computing and on-demand IT.

IBM
www.ibm.com
IBM’s security portfolio provides the security intelligence to help organizations holistically protect their people, infrastructure, data and applications.

RSA
www.rsa.com
RSA is a provider of security, risk and compliance solutions, helping organizations succeed by solving their most sensitive security challenges.

Solutionary
www.solutionsary.com
Solutionary reduces the information security and compliance burden, providing flexible managed security and compliance services.

Symantec
www.symantec.com
A leader in security, storage and management solutions to help secure and manage information and identities.

Additional Sponsors

- HP
- IBM
- F5
- RSA
- Solutionary
- Symantec
- Teleperformance
- Tenable Network Security

Reader Trust Awards

BEST ANTI-MALWARE GATEWAY
WINNER
Cisco for Cisco Web Security
www.cisco.com
Cisco Web Security enables organizations to capture the potential of the web as a collaboration and productivity tool while mitigating risks and protecting users from malware delivered via the web while enforcing acceptable use and data security policies, according to the company. A multilayer threat defense protects users from malware. Web Reputation and Outbreak Intelligence combined with anti-malware engines, provide protection and accuracy against zero-hour threats.

As well, application controls provide visibility and granular controls over Web 2.0 and social networking apps. Reporting and tracking ensure that customers have in-depth visibility and forensics. Integration with Cisco networking and security products, such as the ISR G2 router and AnyConnect Secure Mobilility client, seamlessly protect branch offices, mobile users and devices, however they access the web, the company says. Additionally, choice of appliance, cloud and hybrid deployments provide customers with flexibility to meet the specific needs of their organizations.

Cisco Security Intelligence Operations (SIO) gathers telemetry from 700,000 plus sensors and 600 plus third-party threat intelligence feeds. Cisco SIO delivers web reputation, stopping more than 70 percent of malicious transactions, as well as Outbreak Intelligence, a content-based zero-day threat intelligence feed. Cisco SIO utilizes the massive machine data generated by websites, applications, servers, networks and mobile device.

Cisco Security Intelligence Operations (SIO) gathers telemetry from 700,000 plus sensors and 600 plus third-party threat intelligence feeds. Cisco SIO delivers web reputation, stopping more than 70 percent of malicious transactions, as well as Outbreak Intelligence, a content-based zero-day threat intelligence feed. Cisco SIO utilizes the massive machine data generated by websites, applications, servers, networks and mobile device.

In addition to anti-malware protection, the product includes anti-spam, personal firewall, anti-spyware, host-based intrusion prevention and internet security training. These features work together to provide maximum protection for a complete computing experience.

The ESET solutions’ small footprint and detection method provide effective malware protection without compromising system performance; according to the company. ESET has long been recognized as a leader in proactively detecting and blocking new threats without relying strictly on existing virus signatures. Advanced heuristics extend the standard capabilities of ESET Smart Security and allow detection of a high percentage of new threats.

Overall, for the customer, security is not about collecting data, but rather about separating the wheat from the chaff so their IT staff can take action to mitigate risks.

Finalists 2012

- Bit9 for Bit9 Parity Suite
- ESET for ESET Smart Security
- IBM for IBM Tivoli Endpoint Security and Data Manager
- Sophos for Sophos Endpoint Security and Data Protection v7.7

Best Anti-Malware Management
WINNER
ESET for ESET Smart Security
www.ESET.com
With the rise of high-profile hackers, 2011 has proven to be one of the biggest years for cyber attacks that the online community has ever seen, reaffirming the need for proactive security solutions.

ESET’s Smart Security is a complete security solution produced from the firm’s long-term effort to combine maximum protection with a minimal system footprint. The product has an extremely efficient code base, which eliminates the unnecessary size and extra components found in competitive products. This means faster, more accurate scanning that won’t slow down one’s computer or network, according to the company. ESET Smart Security detects and blocks new, unknown threats for multiple platforms, while providing malware protection.

Finalists 2012

- Bit9 for Bit9 Parity Suite
- ESET for ESET Smart Security
- GFI for GFI VIPRE Anti-virus Business
- IBM for IBM Tivoli Endpoint Manager
- Sophos for Sophos Endpoint Security and Data Protection v7.7

2012 SC AWARDS U.S.
IBM’s cloud security solutions span multiple domains including risk and compliance, application and data security, physical and logical infrastructure security and identity and access management. Taking into account unique challenges of cloud computing – like multitinenancy, virtualization, rapid provisioning and federated identities – IBM has designed security solutions specific to the cloud. Additionally, it has adapted other offerings to meet cloud security needs, including cloud security strategy and assessment services for the development of cloud strategy based on business goals, security requirements and best practices; professional security services for the assessment and penetration testing of cloud applications and infrastructures, assessment and design of identity management controls, cloud based risk/compliance assessment, and policy management; host and network intrusion prevention solutions for the protection of networks and hosts within the cloud infrastructure from attack or misuse; and managed security services, which reduces costs, improves cloud security and assists with compliance through outsourcing management to IBM experts, according to the company.

IBM’s history coupled with experience in developing and delivering its own cloud solutions, such as SmartCloud Enterprise, Lotus Live, and more, are big differentiators, the company says.

Its cloud capabilities span all security domains with the ability to deliver security end-to-end – from strategy and design, to implementation and management, to assessment and continuous monitoring.
 Proofpoint for Proofpoint Enterprise Protection/Enterprise Privacy

Fortinet for Fortinet 100C

Cisco Systems for Cisco IronPort Email Security

Finalists 2012

Cisco Systems for Cisco IronPort Email Security
Fortinet for Fortinet 100C
Proofpoint for Proofpoint Enterprise Protection/Enterprise Privacy
Symantec for Symantec Messaging Gateway 9.5
Webroot for Webroot Email Security Gateway Anywhere

Finalists 2012

Sophos for Sophos Security Gateway
Symantec for Symantec Email Security cloud

WINNER

Sophos for Sophos Security Gateway v8.2

www.sophos.com

The Astaro Security Gateway offers complete UTM protection, and can be installed as either hardware, software or a virtual appliance. For more sophisticated deployment scenarios, the company offers additional Gateway Accessories that enable new functionality for the gateway. The Astaro Security Gateway uses a combination of anti-spam, encryption and anti-virus scanning, such as a reputation service with spam outbreak detection, recipient verification, reverse-DNS and HELO syntax checks, dual independent virus scanners with multiple detection methods and more.

Version 8.2 of Astaro Security Gateway includes several new features, including application control, log management and several other enhancements. These improvements will help organizations protect their network from modern threats, according to the company. It simplifies security by making it easy to deploy and manage while still being powerful enough to protect against email, web, network and web app threats, as well as wireless security.

Astaro says it is the only VMware-ready certified UTM vendor. This distinction allows organizations of all sizes to take advantage of Astaro’s network protection in the deployment model that best fits their organization’s needs. The Astaro Security Gateway also offers an easy-to-use graphical interface that makes administrating the appliances simple. Another advantage is Astaro’s integration of not only network, web and mail subscriptions, but also web application security, next-generation firewall functions, log management, wireless security and Astaro RDM integration.

Barracuda Networks for Barracuda NG Firewall

www.barracudanetworks.com

Barracuda NG Firewall enables customers to take full control over their entire network by integrating Layer 7 application control of rogue applications with full integrated user awareness. The solution optimizes network traffic flow via intelligent adaptive WAN routing, while extend-ing security and application control to every location – be it small offices or large head-quarters. Further, it provides integrated easy-to-manage and full-featured network access control (NAC), and saves considerably on manage-ment overhead via complete, scalable and centralized management of all functions and lifecycle that was built in, according to the company.

While most of these features would be available via the deployment of individual point products, the combined ben-efts – such as vastly reduced administrative overhead, a stabilized network, and a consistent security posture across the whole network – are now available with the Barracuda NG Firewall. The platform has early development roots not only in centralized configuration, policy and reporting, but also in site-to-site WAN traffic management capabilities. The Barracuda NG Firewall is designed to optimize both the availability and performance of the WAN, with lower administrative overhead than competing solutions. Combined with its unique capabilities for large-scale centralized management and intelligent traffic management for site-to-site WAN con-nectivity, the Barracuda NG Firewall is one of the most advanced solutions of its kind at any price.

Trustwave for Trustwave Fraud Prevention

www.trustwave.com

IronKey for IronKey Trusted Access

www.ironkey.com

IronKey’s Trusted Access enables banks to provide their customers with a secure browsing solution for online banking and e-commerce that keeps customers safe on their own PCs, even if they are infected with financial malware. It prevents online fraud by innovating in three layers of technology – a secure portable device, virtualization and a cloud-based secure network. With Trusted Access, banks deliver to clients a customized, secure web browser protected in a fully virtualized, read-only environment tailored to work exclusively with IronKey’s Trusted Network and the bank’s systems to protect online banking sessions from known and unknown crimeware. It also offers trusted bookmarks, a safe way to access websites by using a “whitelist” managed by the bank. When shopping online, the service assures customers that they are accessing an au-thentic site and that payments are not being monitored or tampered with, according to the company.

Barracuda Networks for Barracuda NG Firewall
Check Point Software Technologies for Check Point R75.20
Cisco Systems for Cisco Catalyst 6500 Series ASA Services Module
McAfee for McAfee Firewall Enterprise
Palo Alto Networks for Palo Alto Networks PA-5000 Series

Finalists 2012

Access Denied
The webpage you attempted to visit is not allowed.
For your security, only pages designated by your financial institution may be visited.

Why does this happen?
This can occur if an malware attempt to connect you to a phishing site, or your bank updated deployment the website for use with this device.

Back
Home

Finalists 2012

CA Technologies for CA RiskMapper (formerly CA ArcSight RiskFont)
Entrust for Entrust TransactionGuard
Guardian Analytics for FraudMAP
IronKey for IronKey Trusted Access
Trustwave for Trustwave Fraud Prevention

Reader Trust Awards

BEST EMAIL CONTENT MANAGEMENT

Proofpoint for Proofpoint Enterprise Protection/Proofpoint

Finalists 2012

Sophos for Sophos Security Gateway
Symantec for Symantec Email Security cloud

WINNER

Sophos for Sophos Security Gateway v8.2

www.sophos.com

The Astaro Security Gateway offers complete UTM protection, and can be installed as either hardware, software or a virtual appliance. For more sophisticated deployment scenarios, the company offers additional Gateway Accessories that enable new functionality for the gateway. The Astaro Security Gateway uses a combination of anti-spam, encryption and anti-virus scanning, such as a reputation service with spam breakout detection, recipient verification, reverse-DNS and HELO syntax checks, dual independent virus scanners with multiple detection methods and more.

Version 8.2 of Astaro Security Gateway includes several new features, including application control, log management and several other enhancements. These improvements will help organizations protect their network from modern threats, according to the company. It simplifies security by making it easy to deploy and manage while still being powerful enough to protect against email, web, network and web app threats, as well as wireless security.

Astaro says it is the only VMware-ready certified UTM vendor. This distinction allows organizations of all sizes to take advantage of Astaro’s network protection in the deployment model that best fits their organization’s needs. The Astaro Security Gateway also offers an easy-to-use graphical interface that makes administrating the appliances simple. Another advantage is Astaro’s integration of not only network, web and mail subscriptions, but also web application security, next-generation firewall functions, log management, wireless security and Astaro RDM integration.

Barracuda Networks for Barracuda NG Firewall

www.barracudanetworks.com

Barracuda NG Firewall enables customers to take full control over their entire network by integrating Layer 7 application control of rogue applications with full integrated user awareness. The solution optimizes network traffic flow via intelligent adaptive WAN routing, while extending security and application control to every location – be it small offices or large headquarters. Further, it provides integrated easy-to-manage and full-featured network access control (NAC), and saves considerably on manage-ment overhead via complete, scalable and centralized management of all functions and lifecycle that was built in, according to the company.

While most of these features would be available via the deployment of individual point products, the combined ben-efts – such as vastly reduced administrative overhead, a stabilized network, and a consistent security posture across the whole network – are now available with the Barracuda NG Firewall. The platform has early development roots not only in centralized configuration, policy and reporting, but also in site-to-site WAN traffic management capabilities. The Barracuda NG Firewall is designed to optimize both the availability and performance of the WAN, with lower administrative overhead than competing solutions. Combined with its unique capabilities for large-scale centralized management and intelligent traffic management for site-to-site WAN connectivity, the Barracuda NG Firewall is one of the most advanced solutions of its kind at any price.

Trustwave for Trustwave Fraud Prevention

www.trustwave.com

IronKey for IronKey Trusted Access

www.ironkey.com

IronKey’s Trusted Access enables banks to provide their customers with a secure browsing solution for online banking and e-commerce that keeps customers safe on their own PCs, even if they are infected with financial malware. It prevents online fraud by innovating in three layers of technology – a secure portable device, virtualization and a cloud-based secure network. With Trusted Access, banks deliver to clients a customized, secure web browser protected in a fully virtualized, read-only environment tailored to work exclusively with IronKey’s Trusted Network and the bank’s systems to protect online banking sessions from known and unknown crimeware. It also offers trusted bookmarks, a safe way to access websites by using a “whitelist” managed by the bank. When shopping online, the service assures customers that they are accessing an authentic site and that payments are not being monitored or tampered with, according to the company.

Barracuda Networks for Barracuda NG Firewall
Check Point Software Technologies for Check Point R75.20
Cisco Systems for Cisco Catalyst 6500 Series ASA Services Module
McAfee for McAfee Firewall Enterprise
Palo Alto Networks for Palo Alto Networks PA-5000 Series

Finalists 2012

Sophos for Sophos Business Class Email
GFI Software for GFI MailSecurity Complete
McAfee for McAfee Email Protection
SoniWALL for SoniWALL Email Security Appliance 8300
Sophos for Sophos Security Gateway
Symantec for Symantec Email Security cloud

WINNER

Sophos for Sophos Security Gateway v8.2

www.sophos.com

The Astaro Security Gateway offers complete UTM protection, and can be installed as either hardware, software or a virtual appliance. For more sophisticated deployment scenarios, the company offers additional Gateway Accessories that enable new functionality for the gateway. The Astaro Security Gateway uses a combination of anti-spam, encryption and anti-virus scanning, such as a reputation service with spam outbreak detection, recipient verification, reverse-DNS and HELO syntax checks, dual independent virus scanners with multiple detection methods and more.

Version 8.2 of Astaro Security Gateway includes several new features, including application control, log management and several other enhancements. These improvements will help organizations protect their network from modern threats, according to the company. It simplifies security by making it easy to deploy and manage while still being powerful enough to protect against email, web, network and web app threats, as well as wireless security.

Astaro says it is the only VMware-ready certified UTM vendor. This distinction allows organizations of all sizes to take advantage of Astaro’s network protection in the deployment model that best fits their organization’s needs. The Astaro Security Gateway also offers an easy-to-use graphical interface that makes administrating the appliances simple. Another advantage is Astaro’s integration of not only network, web and mail subscriptions, but also web application security, next-generation firewall functions, log management, wireless security and Astaro RDM integration.
As organizations move through the process of hiring, transferring, acquiring and/or restructuring, it is difficult to keep track of ever-changing users and the access they have to business applications. With pressures to improve operational efficiencies, reduce costs, mitigate risks and ease compliance, IT organizations are challenged to limit access based on users’ fluctuating access needs, as they leave, efficiently managing the multitude of threats while simplifying their security deployment and reducing costs. The Check Point IPS Software Blade helps customers increase their security, reduce their security complexity, while also reducing security costs. The business and technical advantages include unmatched flexibility and expandability. The Software Blade Architecture and the IPS Software Blade allow customers to access the corporate network – with an expectation that IT will support them. And since many of these devices are owned by the individual, IT has no control over what resides on the device, and it has little-to-no insight into the security posture of the device, prior to connection. Cisco AnyConnect Secure Mobility Solution addresses these challenges by providing users with secure remote access to the corporate network using their device of choice, regardless of their physical location, to easily and securely use the applications and information they need to do their jobs. Cisco AnyConnect Secure Mobility scales to 5 Gbps of VPN throughput or 100,000 users leveraging Cisco ASA security appliances, or Cisco ASR or ISR routers, for comprehensive secure connectivity. In addition, AnyConnect uses Cisco Ironport Web Security Appliances or Cisco ScanSafe in the cloud to integrate web security. Always-on connectivity and the intelligence of AnyConnect automatically selects the most optimal network access and adapts its tunneling protocol, even accommodating latency sensitive traffic. This keeps mobile workers efficient and productive as they roam between locations, according to the company.
PGP Whole Disk Encryption works together with a range of encryption solutions from Symantec, ensuring that an organization can address immediate needs for data protection straight away, and address new needs over time. It offers broad platform support, including Windows, Windows Server 2K8 and 2K3, Mac OS X, Linux Ubutu, CentOS, and Red Hat. Further, strong management tools offer key management, and consolidated security management console with Symantec Protection Center. The tool provides advanced support for Intel encryption technology. It works with Intel vPro for anti-theft and deprovisioning, and supports AES-NI crypto acceleration in all OSs. In addition, it provides validations/certifications with the toughest cryptographic and security standards, including EAL 4 plus, FIPS 140-2, plus DIPCOG approved and CAPS approved.

Winners

PGP Whole Disk Encryption from Symantec for PGP Whole Disk Encryption from Symantec

Winner

Entrust for Entrust IdentityGuard

www.entrust.com

Entrust IdentityGuard enables organizations to implement strong authentication to employee, partner, contractors and authorized third parties – and only when it makes sense. It offers one of the widest ranges of strong authentication options on the market today, which includes physical or non-physical approaches, and can be transparent to users or take advantage of existing mobile devices, according to the company. It represents a more affordable approach to deploying a wide range of authentication capabilities at a fraction of the cost of traditional, single-purpose solutions. It provides flexibility to tailor authentication to user preference, transaction risk and cost. And, it minimizes user impact, enabling a choice of authentication methods, only performing authentication when needed to reduce risk.

Reader Trust Awards

Best Mobile/Portable Device Security

Winner

ForeScout Technologies for ForeScout CounterACT

www.forescout.com

The ForeScout Counter- ACT NAC solution is easy, integrated, interoperable and automated – delivering real-time visibility and broad control over all users, devices, OSs and applications before appropriate access to network resources is granted – without requiring agents and using existing infrastructure. ForeScout’s network-based NAC delivers rich user and device classification and built-in and extensible policies to determine who the user is (and what directory group association), what is the device, what is the configuration and security posture of the device (active and current client security, patches, allowed applications and software, and more), as well as when and what network resources are being requested. Available as a scalable appliance or virtual appliance family, CounterACT’s built-in advanced device classification, infrastructure plug-ins, 802.1x support, policies, guest registration, actions, remediation and reporting address evolve NAC requirements and accelerate time-to-value, according to the company. CounterACT offers rich network access control, guest networking, endpoint compliance, mobile security, remediation and reporting. It is fully integrated and interoperable, supporting the majority of network and infrastructure. It does not require multiple components to manage, or predefined knowledge of the endpoint. As well, there is no need to change or update network or endpoint devices, to deploy agents, nor manage 802.1x devices. CounterACT offers robust network discovery and automated device classification with rich device fingerprinting.

2012 SC Awards U.S.
Reader Trust Awards
BEST SECURITY INFORMATION/EVENT MANAGEMENT (SIEM) APPLIANCE

WINNER
HP for HP ArcSight Express
www.hp.com
HP ArcSight Express combines SIEM, log management and user activity monitoring on a single appliance, moving beyond perimeter security to monitor what truly matters to HP ArcSight customers, according to the company. It collects from any data source, consolidates the information for maximum storage efficiency, and correlates the events in multiple dimensions, including, identity, vulnerability, asset, time, statistical calculations, pattern, and other events to detect the advanced threats that organizations face in a post-perimeter world.

ArcSight Express does three things: data collection, consolidation and correlation. It supports data collection from more than 300 commercial and open source products, and has a “flex” connector architecture that is used by customers to connect to thousands more data sources to establish full visibility into their environments. All of the connectors are virtualization and cloud ready.

The tool’s consolidation architecture provides 10:1 compression of all events, significantly increasing the data that can be monitored and stored on a single appliance. As attacks gate over longer periods of time and compliance requirements tighten, this functionality is critical to helping customers stay secure and compliant, according to the company. HP ArcSight Express can pull information from directories and identity management systems and use that data to monitor user activity, even when logs show an IP address or shared account credentials, according to the company.

Reader Trust Awards
BEST UTM

WINNER
Fortinet for FortiGate-60C
www.fortinet.com
The FortiGate-60C multi-threat security appliance offers unmatched performance, flexibility and security for remote, branch or small office networks. The appliance integrates firewall, IPS and SSL VPN, anti-virus, anti-spam, intrusion prevention, web filtering, data leakage prevention (DLP), application control, SSL inspection, endpoint NAC and vulnerability management into a single device at a single price. And, dynamic threat updates are provided by FortiGuard Labs.

The appliance couples high-performance hardware with an internal data storage and innovative expansion options, such as wireless broadband support, on one appliance. It is Fortinet’s most prolific network security appliance in the field.

No other device in its price range offers the speed (1Gbps firewall throughput), breadth and depth of protection (FortiGuard) as the FortiGate-60C, according to the company. Custom processors maximize throughput with one or multiple security services – blocking unauthorized access and eliminating unwanted traffic or threatening attacks. Virtual Domains (VDOMs) enable a single FortiGate-60C to function as multiple independent virtual FortiGate systems, enabling multiple uses for a variety of applications and user access with different policies on one box. Each VDOM contains its own virtual interfaces, security profiles, routing table and administration.

Finally, the FortiASIC processors in the FortiGate-60C allow organizations to deploy unified threat management functionality without sacrificing network performance.

Reader Trust Awards
BEST VULNERABILITY MANAGEMENT TOOL

WINNER
Rapid7 for NeXpose Enterprise
www.rapid7.com
As the number of attacks and vulnerabilities continue to rise, security professionals need real security risk intelligence to help them prioritize threats and re-mediate the greatest risks first.

Rapid7’s web-based vulnerability management product, NeXpose, leverages one of the largest vulnerabilities databases to identify vulnerabilities across networks, operating systems, databases and web applications.

NeXpose manages the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation. Risk is classified based on real exploit intelligence combined with industry standard metrics, such as CVSS, as well as temporal and weighted risk scoring. NeXpose provides a detailed, sequenced remediation roadmap with time estimates for each task. NeXpose is used to help organizations improve their overall risk posture and security readiness, as well as to comply with mandatory regulations, including security requirements for PCI, HIPAA, ARRAHITECH Act, FISMA, Sarbanes-Oxley and NERC CIP.

NeXpose’s unique capabilities for complex IT environments earned the highest possible ratings for vulnerability management ability from both Gartner and Forrester in recent evaluations. According to Forrester, Rapid7 is “The only vendor in this evaluation whose scanning capabilities can handle Ajax and Web 2.0 technologies.” In fact, NeXpose is used to help organizations improve their overall risk posture and security readiness, as well as to comply with mandatory regulations, including security requirements for PCI, HIPAA, ARRAHITECH Act, FISMA, Sarbanes-Oxley and NERC CIP.

NeXpose’s unique capabilities for complex IT environments earned the highest possible ratings for vulnerability management ability from both Gartner and Forrester in recent evaluations. According to Forrester, Rapid7 is “The only vendor in this evaluation whose scanning capabilities can handle Ajax and Web 2.0 technologies.” In fact, NeXpose is used to help organizations improve their overall risk posture and security readiness, as well as to comply with mandatory regulations, including security requirements for PCI, HIPAA, ARRAHITECH Act, FISMA, Sarbanes-Oxley and NERC CIP.

NeXpose’s unique capabilities for complex IT environments earned the highest possible ratings for vulnerability management ability from both Gartner and Forrester in recent evaluations. According to Forrester, Rapid7 is “The only vendor in this evaluation whose scanning capabilities can handle Ajax and Web 2.0 technologies.” In fact, NeXpose is used to help organizations improve their overall risk posture and security readiness, as well as to comply with mandatory regulations, including security requirements for PCI, HIPAA, ARRAHITECH Act, FISMA, Sarbanes-Oxley and NERC CIP.

NeXpose’s unique capabilities for complex IT environments earned the highest possible ratings for vulnerability management ability from both Gartner and Forrester in recent evaluations. According to Forrester, Rapid7 is “The only vendor in this evaluation whose scanning capabilities can handle Ajax and Web 2.0 technologies.” In fact, NeXpose is used to help organizations improve their overall risk posture and security readiness, as well as to comply with mandatory regulations, including security requirements for PCI, HIPAA, ARRAHITECH Act, FISMA, Sarbanes-Oxley and NERC CIP.

NeXpose’s unique capabilities for complex IT environments earned the highest possible ratings for vulnerability management ability from both Gartner and Forrester in recent evaluations. According to Forrester, Rapid7 is “The only vendor in this evaluation whose scanning capabilities can handle Ajax and Web 2.0 technologies.” In fact, NeXpose is used to help organizations improve their overall risk posture and security readiness, as well as to comply with mandatory regulations, including security requirements for PCI, HIPAA, ARRAHITECH Act, FISMA, Sarbanes-Oxley and NERC CIP.

NeXpose’s unique capabilities for complex IT environments earned the highest possible ratings for vulnerability management ability from both Gartner and Forrester in recent evaluations. According to Forrester, Rapid7 is “The only vendor in this evaluation whose scanning capabilities can handle Ajax and Web 2.0 technologies.” In fact, NeXpose is used to help organizations improve their overall risk posture and security readiness, as well as to comply with mandatory regulations, including security requirements for PCI, HIPAA, ARRAHITECH Act, FISMA, Sarbanes-Oxley and NERC CIP.

NeXpose’s unique capabilities for complex IT environments earned the highest possible ratings for vulnerability management ability from both Gartner and Forrester in recent evaluations. According to Forrester, Rapid7 is “The only vendor in this evaluation whose scanning capabilities can handle Ajax and Web 2.0 technologies.” In fact, NeXpose is used to help organizations improve their overall risk posture and security readiness, as well as to comply with mandatory regulations, including security requirements for PCI, HIPAA, ARRAHITECH Act, FISMA, Sarbanes-Oxley and NERC CIP.
traffic in real-time, categorizing dynamic social web content/threats, plus preventing data theft. ACE and Webense ThreatSensor inspect three to five billion pieces of content from more than 50 million sources daily. Proactive social web content analysis/controls enable policies for social media sites to address detailed functional controls. Additional functionalities address viral videos, posts on social networks, or制动 with advanced video and entertainment videos, and limit access to sites using dynamic DNS.

Webense Web Security Gateway provides a single management console and a single policy that manages appliance and cloud/SaaS defenses for users in the office or remotely. This is part of the TRITON solution that unifies web, email and data security across both on-premise and cloud platforms for a lower cost, according to Webense.

As well, its customer loyalty is strong with nearly 100 percent retention rate. More than 70 percent of customers license multiple applications, and more than 10 percent of customers are repeat buyers.

Agilance's commitment to making risks visible, measurable and actionable extends beyond delivering comprehensive GRC solutions. Agilance offers a variety of services from training and implementation to ongoing architecture assessment. Also, its highly trained customer service team delivers consulting services for project planning and analysis, implementation, onsite and remote training, and custom development, according to the company. Its support programs maximize the performance and availability of mission-critical GRC resources, including the visioning of technical support engineers in centers worldwide, which routinely averages 8:11 (out of 10) in industry surveys. Offerings include Standard, Premium (unlimited 24/7) and Mission Critical (fastest, designated account manager). In fact, the company's customer support recently won the Association of Support Professionals' 2011 "Best Web Support" award and achieved Service Capability & Performance (SCP) Support Standard certification.

"We've worked with many different vendors where it was hard to get a hold of anybody to get a question answered and find people to help us with our problem," says Mark Choi, manager of instructional technology, Bellevue School District. "It was very reassuring that I could just pick up the phone and call someone at Webense to get help right away, and get a problem resolved within a reasonable amount of time. Everyone I spoke with was very knowledgeable of the product and had an intelligent answer." Webense invests in research and development at six worldwide facilities.
eCert systems.com

eCert’s offerings include its Email Protection Identity Cert (EPIC) and the FS-ISAC and BITS Trusted Email Registry. Launched in April 2010, eCert’s offerings continue to advance with multiple enhancements to provide intelligence, protection and trust for email, according to the company. The eCert EPIC service operates as an internet-based registry of email domain information that publishes monitoring and security instructions to receiving networks, and simultaneously collects and analyzes traffic information gathered from those networks. There is no installed hardware or software, so the ease of use of both services has increased the customer base, according to the company. eCert offers 24/7/365 enterprise support for its clients. Customer service includes complete deployment, testing and support services to members. This includes relationship and legal management with receivers (ISPs), project management, authentication and service deployment consulting, tools, data and threat analysis, trend reporting and metrics.

The company regularly hosts industry summits with leading financial institution partners, internet service provider (ISP) and security partners to develop an ongoing roadmap to protect services for online communications, too. eCert hosts these summits every three months to ensure that all relevant, critical and topical issues in the industry are being addressed, according to eCert.

To improve online communications and restore trust and safety to email, in 2011, eCert donated its intellectual property and key specifications for the development of open industry standards to promote a scalable, industry-wide email security solution.

MANDIANT

www.mandiant.com

MANDIANT’s people and product approach to incident response differentiate the company from any other firm and has contributed to the company’s dramatic growth over seven years, according to the company. MANDIANT’s elite force of incident responders and forensic investigators bring to each breach investigation a unique blend of technical and investigative experience and offer leading incident response, malware analysis and incident response program development.

It is investing significantly in the delivery of next-generation threat detection and response through MCERT, the MANDIANT Computer Incident Response Team, which combines MANDIANT’s experience in advanced threat detection and response, exposure to diverse threat intelligence, revolution- ary technology, and some of the best incident responders in the business, according to the company. This combination provides customers with effective incident insight – from host to network – along with actionable intelligence.

MANDIANT offers a range of options for products and services: one-on-one phone support, a secure portal for customer-only access, and an interactive, web-based user forum for sharing company-client discussions/Q&A. MANDIANT research, product and service updates, and ‘freshness levels’ assigned to relevant topics and issues.

As well, clients and other industry end-users benefit from MANDIANT’s detailed emergency incident response web page. This comprehensive, publicly available summary of incident response best practices helps customers and the broader industry prepare for and mitigate breach events.
The SANS Institute provides hands-on, intensive, immersion training designed to help students master the practical steps necessary for defending systems and networks. Beginners to seasoned experts can find a SANS course to fit their technical needs. Every SANS course is written and taught by top experts who are real-life practitioners in their respective fields. Courses are either job- or skill-based and cover general security, intrusion detection, incident handling, forensics, penetration testing, application security, secure coding, management and auditing.

SANS also features a variety of free resources for security professionals: The Internet Storm Center is a free analysis and warning service for internet users and organizations. Additionally, the SANS Reading Room contains two thousand computer security white papers. Also offered are live webcasts covering information security topics, and four newsletters covering high-level executive summaries and alerts.

According to SANS, it differs from other training programs in four important ways: course content, instructors, methods of delivery and commitment to the community. Most importantly, it also promises immediate practical application: “You will be able to put what you learn into practice the day you return to the office.”

SANS authors and instructors are authors of best-selling information security books, as well as course authors. They also are quoted in the media and information-security-related articles for publications and websites. Overall, SANS courses empower students with the knowledge they need to protect their systems and data.

# Winning Awards

**WINNER**

**SANS Institute**

**WINNER**

**Stephen Scharf, global CISO, Experian**

Stephen Scharf, the global chief information security officer for Experian, has more than a decade of experience building strong IT security teams. He understands his role as the face of IT security and that this role requires him to present the highest standard of credibility and integrity to his peers and the organization as a whole. Scharf joined Experian, a company with more than 15,000 employees in 41 countries, as its first global CISO.

As a strong proponent of knowledge management, he continuously looks for best practices in IT security and applies these to the global environment in an effective and efficient manner, according to Experian. Scharf strives constantly to stay updated on the latest security threats facing the industry, and consistently shares this knowledge with his team – integrating it into team building, cross-training among various business groups, and problem solving – and leverages feedback from the team with the broader organization to ensure security goals are aligning with business needs.

Scharf’s motto is to “treat security as a partnership.” IT security is intimately involved in every part of Experian’s operations. As a result, he works closely with all areas of the business – from developers and engineers to his colleagues in IT and the executive team – and dedicates himself to understanding their concerns.

Scharf is steadfast on remaining cognizant of everything across the security portfolio – from users on the network, application security, viruses and more – and works with the executive and IT teams to create a solution that benefits all aspects, while maintaining the focus on overall business needs.

**WINNER**

**Douglas Maughan, division director, Cyber Security Division and DHS Science and Technology Directorate, U.S. Department of Homeland Security**

Maughan and his team is to develop the product so it can make it to market help accomplish exactly that. And there have been numerous HSARPA success stories. Since 2004, SIBR has provided Phase Two funding rounds for 22 companies, resulting in 2012 SEGRAR success stories for the Federal Cybersecurity Advanced Research Projects Agency (HSARPA), part of the Science and Technology Directorate, is trying to isolate breakthrough innovations. One of the responsibilities of Maughan and his team is to seed small businesses with capital, then leverage new innovation and transition to the marketplace.

Five companies win Phase One funding, which totals about $100,000 and is used to create a prototype. If the design is promising enough, one or two of those firms receive another $750,000 to further develop the product so it can be commercialized.

Some rookie companies actually prefer to deal with government rather than seek support from angel or private investors. “Not all small entrepreneurs know how to navigate the venture landscape,” Maughan says.

He adds that the program, Small Business Innovative Research, is done to not only help those fledgling organizations that need a financial boost, but also to carry on a primary mission of DHS: to protect critical infrastructure. The hope, he says, is that the products that make it to market help accomplish exactly that. And there have been numerous HSARPA success stories. Since 2004, SIBR has provided Phase Two funding rounds for 22 companies, resulting in eight commercial products currently available. Three of the winning firms have carried their maturity all the way to acquisition.

Maughan points to an eight-employee business, Komoku, founded in 2004. The firm, which sprang out of the University of Maryland, built a toolkit detection technology. “By the time we hit 2007, malware was very prevalent, and they were being courted by McAfee, Symantec and Microsoft,” Maughan recalls.

Beyond leading the charge to make certain that innovation doesn’t die, Maughan’s team is involved with a number of other initiatives. His department is the sponsor and driving force behind the HOST program, whose mission is to investigate open security methods, models and technologies and identify viable and sustainable approaches that support national cyber security objectives. To achieve this mission, HOST is leading efforts of discovery, collaboration and seeding development in open source software and practices that produce a measurable impact. During 2013, DHS S&T released “Mobile Device Forensics,” to support research and development by small businesses to support law enforcement requirements.

No matter what the drivers, Douglas Maughan is hopeful that innovation in cybersecurity has become a discipline in its own right. In fact, technology officials in Washington recently announced a partnership among Maughan’s division, the National Institute of Standards and Technology (NIST) and the Financial Services Sector Coordinating Council, which represents banks, insurance companies and investment firms. The goal of the alliance is to “accelerate the deployment of network test beds for specific use cases that strengthen the resiliency, security, integrity and usability of financial services and other critical infrastructures’ functions, processes and people,” according to blog post written by federal CTO Aneesh Chopra, and Howard Schmitt, national cybersecurity coordinator.
By now, the process is almost routine. A major technology or defense company announces a serious security breach and suspicion quickly falls on China-based attackers. While U.S. officials have been coy about naming the culprit, preferring to say only that a nation-state was most likely behind the attacks, they have recently been more willing to raise the heat on Beijing by calling China out. So far, this naming and shaming does not seem to have had any effect on the calculus of Chinese hacking, and this is unlikely to change in the near-term. As a result, companies will have to continue to remain vigilant and take defense into their own hands.

The motivations for Chinese hacking are not mysterious. Government officials there are unhappy with China being the “factory to the world”—it is labor- and energy-intensive and damages the environment—and desperately want to move the country into higher-value sectors. To do this, China has significantly ramped up research and development spending, but it has also relied on foreign industrial espionage directed at high-tech companies. Hackers have also targeted the negotiation strategies and financial information of energy and banking companies.

Some types of hacking also act as a societal release valve, venting nationalistic feelings. Chinese officials, for example, turned a blind eye when hackers defaced the Nobel Foundation website after rights activist Liu Xiaobo won the Nobel Peace Prize in October 2010. Finally, open-source Chinese defense writings stress the importance of cyber attacks—both in the opening stage of a military conflict and as a deterrent to “outside powers.”

It should also be noted that the Chinese see a great deal of hypocrisy in Washington’s actions in cyber space. As Chinese officials are quick to note, it was the United States that first set up a cyber command—thus, in their view, militarizing cyber space.

What could shift Chinese behavior? Chinese analysts currently see the United States as more vulnerable to attacks, more economically and militarily dependent on networks than China, but that balance may be shifting. Cyber crime is already threatening the Chinese economy—the country suffered close to 500,000 attacks in 2011, according to Chinese sources—and as the People’s Liberation Army modernizes, it becomes more dependent on communication and computer networks. A more vulnerable China may be a more restrained China.

There are also competing interests within the Chinese government. While some factions may see economic espionage as providing a technology boost, other groups may worry that the risk to the bilateral relations with the United States is too high. In addition, for image and status concerns, Beijing traditionally does not like being on the outside of international agreements. Once there is an established set of international norms of state behavior in cyber space, China may slowly gravitate toward them.

Assembling an international consensus on cyber standards, influencing internal debates and waiting for China to become more vulnerable to cyber attacks are all long-term strategies with an uncertain chance of success. With no international agreement on the horizon, companies need to do a better job of protecting intellectual property and trade secrets. They should take inventory of all data stored digitally, remove critical information from vulnerable servers, and limit the time hackers are able to spend on networks by deploying intrusion systems. Chinese hacking is not going away soon.

Adam Segal is the Ira A. Lipman senior fellow at the Council on Foreign Relations. He blogs at Asia Unbound, and you can follow him on twitter @adschina.

Chinese hacking may slow, but...
World’s No. 1
Antivirus and Internet Security

ESET leads the industry in the consecutive number of “VB100” awards from Virus Bulletin testing organization.

Virus Bulletin Awards  Success ratio (%)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>25</th>
<th>50</th>
<th>75</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESET</td>
<td></td>
<td></td>
<td>97</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>93</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td>92</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sophos</td>
<td>78</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kaspersky</td>
<td>76</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GDATA</td>
<td>73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McAfee</td>
<td>68</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TrendMicro</td>
<td>67</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Selected Antivirus Vendors (not a complete list)

And the best keeps getting better—IT experts everywhere agree.

© 2012 ESET. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET. All other names and brands are registered trademarks of their respective companies.