FEATURES:

EMPLOYEE BENEFITS

A smarter worker is a more secure worker, says Theresa Masse, CISO, state of Oregon

It’s high time
Data from a new commission report reveals it is time for a nationally enforced data breach reporting mandate.

IPS grows up
The technology has evolved, but some say new features are not enough for today’s attacks
REGULARS
4 Editorial  When less isn’t more
8 Threat report  Saudi Arabia was top producer of zombie IP addresses
10 Threat stats  The biggest increases in month-over-month zombie activity occurred in China and Vietnam
12 Update  The Canadian government has unlocked $155 million in funding to bolster cyber security
13 Debate  The cyber security executive order is a step in the right direction
14 Two minutes on… The resurgence of security IPOs
15 Skills in demand  Security pros with database development training are needed
16 From the CSO’s desk  A trustworthy mobility program, by Michael Scovetta, director of advanced technology at a large media company
17 Letters  From the online mailbag
18 Opinion  No more trusted endpoints, by Conrad Constantine, research engineer, AlienVault
49 Calendar  A guide to upcoming IT security shows, events and courses
50 Last word  Take to the offense with intel, by Christopher Harrington, consulting security engineer, EMC

FEATURES
20 Employee benefits  Security pros must realize that a smarter worker is a more secure worker, says Theresa Masse, CISO, state of Oregon.
24 Waking the sleeping giant  Stuxnet was a game changer for SCADA operations, but control systems that run the nation’s infrastructure are still at risk.
26 IPS grows up  The intrsion prevention system has evolved, but experts dispute whether it offers enough to thwart today’s attacks.
29 Storms ahead  The cloud presents new challenges in protecting data.
32 On-the-go defense  Mobile users downloading apps onto devices is cause for concern.
48 The future is now  Security professionals gathered on Oct. 11 for the fifth-annual SC Congress New York.

PRODUCT REVIEWS
37 Product section  There is a new network architecture paradigm that distributes protection throughout the enterprise, as well as the applications running on it.
38 Group Test: Database and application security  While we did not see a lot of encryption in this set of products, these tools can severely curtail the complexity of attacks against applications.
47 First Look: TMC from TITUS  A creative approach to message classification and enforcement.
When less isn’t more

Among the some 400 attendees at last month’s SC Congress New York, fears handballed across various spectrums. Dealing with cloud service providers slow to address customers’ security needs or the threats brought to companies because of mobile devices or BYOD (bring-your-own-services) were quite the hot topics. As well, supply-chain attacks from politically hostile countries and public-private partnering made the list of concerns discussed during speaker sessions, keynotes and social hangs.

Although information security pros hitting the one-day conference and expo left it armed from either presidential candidate on how they would help organizations to concentrate on criminals, nation-states and other adversaries the internet. Sure, information sharing about order. And that’s mighty ironic given how reli-

ation may be piecing together an executive — with the exception that the Obama admin-

istration could step up a from either presidential candidate on how they intend to do so when it comes to cyber security – with the exception that the Obama admin-

istration may be piecing together an executive order. And that’s mighty ironic given how reli-

ant the country’s economy is on technology and the internet. Sure, information sharing about the occurrence of attacks, threats from cyber criminals, nation-states and other adversaries would help organizations to concentrate on weaker areas of their infrastructures. However, when the government seeks out private entities’ intelligence and then fails to provide some of their own because it’s ‘classified’ and all, that long-touted two-way street quickly crumbles.

Then there’s the bosses…No doubt, budgets are tight. But, they’re bound to get tighter if a company falls victim to a massive identity theft that leaves customers running to competi-

tors and has the victimized company paying government fines, incident response costs and credit-check services. In failing to underestimate the importance of proper support for security, privacy and compli-

ance endeavors is to become the next my-business-is-clueless headline. And I can’t think of one executive board member, CEO, corporate attorney or PR specialist who would look forward to that.

So think about bringing your CEO to SC Congress Chicago on Nov. 8. They might actually become a little more convinced that more money and staff for you would be a good thing – for both them and the companies they oversee.

Information security pros have an overload of issues to sort out...

Companies aren’t short on data. In fact, with the average large business storing more than 200 terabytes, companies have more than enough data to tell them who is buying their product, as well as how, when and where the buying happens.

DATA’S NEW VOICE.

Today, however, customers expect a company to know why they’re buying. Or why they aren’t. Because when a company knows what motivates customers, it can serve them better.

The good news is such data exists, just not in the columns, rows, reports and purchase histories we’re used to. It’s called big data, and it comes from tweets, videos, clickstreams and other unstructured sources. It’s the data of desire. And today, we have the technology and tools to make sense of it.

So now, instead of learning which customers it has lost, a company can learn which customers it might lose and present timely offers or products motivating those customers to stay. Using IBM Smarter Analytics to identify which customers were most likely to switch to another

SMARter TECHNOLOGY for A SMARTER PLANet

"For the first time, we can decide which promotions to run based on facts rather than gut feel!"

Patrick Neesley
Chief Business Officer
Citizens Nation Division of Commerce

THE POWER OF BIG DATA.

IBM—software, systems and
 Enter Smarter Analytics from IBM—software, systems and

communications carrier, XO Communications was able to predict likely customer defections within 90 days, reducing churn by 35 percent the first year.

With IBM Smarter Analytics, companies are gathering big data and using it to ask—and answer—smarter questions about what their customers really want. ibm.com/usingbigdata

"Let’s build a Smarter Planet."

© International Business Machines Corporation 2012.
A recent study on internet crime found that publicly traded Canadian companies experienced 50 percent more cyberattacks in 2011 than in the previous year. While the Harper government considers a number of new regulations, such as the so-called “lawful internet access” law, many of Canada’s small internet service providers are concerned that proposed federal legislation could drive them out of business. We’ll take a sweeping survey of what is being discussed in Canadian security circles and what companies can do to maximize protection of corporate assets.

Mobile security

Safeguarding handheld devices used by business executives is a constant trial—one that rarely is satisfactorily remedied. We offer solutions.

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.

NEXT MONTH

Dec. 4 eSymposium in Canada: Data security

A recent study on internet crime found that publicly traded Canadian companies experienced 50 percent more cyberattacks in 2011 than in the previous year. While the Harper government considers a number of new regulations, such as the so-called “lawful internet access” law, many of Canada’s small internet service providers are concerned that proposed federal legislation could drive them out of business. We’ll take a sweeping survey of what is being discussed in Canadian security circles and what companies can do to maximize protection of corporate assets.

ON DEMAND

Data security

Many leading CSOs at various conferences this year bemoaned the need for organizations to have their security controls follow and protect their most important data assets, rather than the network. So, just how is this best achieved?

Mobile security

Safeguarding handheld devices used by business executives is a constant trial—one that rarely is satisfactorily remedied. We offer solutions.

FOR MORE INFO

For details on SCWC 24/7 events, please contact Natasha Mull at natasha.mull@haymarketmedia.com.

For sponsorship opportunities, please contact Mike Alessie at mike.alessie@haymarketmedia.com.

For more information, please contact Samantha Amoroso sales campaign manager, SC Magazine samantha.amoroso@haymarketmedia.com 646-638-6021

But, it doesn’t have to be so daunting. Not with the launch of SC MarketScope. This new site, brought to you by SC Magazine, is the place for purchasing IT security products and services. SC MarketScope is the first stop for key decision-makers.

Features include:

1. Vendor overviews
2. Reviews of products/services
3. Expert advice and opinion from IT security contributors and columnists (exclusive to SC MarketScope)
4. Lead generation

We’re live! Visit us at www.scmarketscope.com
Saudia Arabia top producer of zombie IP addresses
For the period reported, the EMEA region (Europe, Middle East, Africa) was the leading source of all zombie IP addresses. Of the countries making up the EMEA, Saudi Arabia was the top producing country. For the other regions the top producers were Brazil in South America, the United States in North America and India in the Asia-Pacific region. Source: Symantec.
Hackers claimed they obtained 12 million Apple Unique Device Identifiers (UDIDs).

**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>unicom-cn</td>
<td>115</td>
</tr>
<tr>
<td>2</td>
<td>chinanet-j</td>
<td>85</td>
</tr>
<tr>
<td>3</td>
<td>chinanet-gd</td>
<td>83</td>
</tr>
<tr>
<td>4</td>
<td>hinet.net</td>
<td>66</td>
</tr>
<tr>
<td>5</td>
<td>tt.net.tr</td>
<td>63</td>
</tr>
<tr>
<td>6</td>
<td>ovh.net</td>
<td>61</td>
</tr>
<tr>
<td>7</td>
<td>iliad.fr</td>
<td>53</td>
</tr>
<tr>
<td>8</td>
<td>comcor.ru</td>
<td>52</td>
</tr>
<tr>
<td>9</td>
<td>hostpac.net</td>
<td>48</td>
</tr>
<tr>
<td>10</td>
<td>telefonica.com.ar</td>
<td>48</td>
</tr>
</tbody>
</table>

The networks listed knowingly provide service to spam gangs and ignore reports from anti-spam systems and internet users.

Source: The Spamhaus Project

**Top breaches in September**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple Cupertino, Calif.</td>
<td>Hackers linked to Anonymous claimed to have obtained Apple Unique Device Identifiers (UDIDs). Apple said it plans to discontinue use going forward.</td>
<td>1,000,000 records posted</td>
</tr>
<tr>
<td>University of Miami Health System Miami</td>
<td>Two University of Miami Hospital employees were using patient registration sheets to inappropriately access personal information.</td>
<td>64,846</td>
</tr>
<tr>
<td>Feinstein Institute for Medical Research Manhasset, N.Y.</td>
<td>A laptop stolen from the car of a contractor contained personal information of current and former patients.</td>
<td>13,000</td>
</tr>
</tbody>
</table>

Total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005: **563,857,193**

(As of Oct. 15)

Source: Privacy Rights Clearinghouse (data from a service provided by DataLossDB.org, hosted by the Open Security Foundation)

**SMS spam**

Volume by month for each region

<table>
<thead>
<tr>
<th>Region</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific</td>
<td>5.08%</td>
</tr>
<tr>
<td>Europe</td>
<td>2.48%</td>
</tr>
<tr>
<td>Africa &amp; Middle East</td>
<td>1.78%</td>
</tr>
<tr>
<td>North America</td>
<td>1.08%</td>
</tr>
<tr>
<td>South America</td>
<td>761.4M</td>
</tr>
</tbody>
</table>

**Zombie IPs**

Global distribution

- Brazil 8.2%
- India 20.3%
- Other South America 4.1%
- Other North America 3.5%
- Other Europe 12.6%
- Other Asia 16.4%
- China 7.2%
- Iran 2.8%
- Peru 2.8%
- Russia 4.3%
- Vietnam 6.1%

The biggest increases in month-over-month zombie activity occurred in China and Vietnam, while the largest decreases occurred in Argentina, Germany and “other” Asian nations.

Source: Commtouch Software Online Labs

**Internet dangers**

Top 10 threats

<table>
<thead>
<tr>
<th>Name</th>
<th>Movement</th>
<th>Data first observed</th>
<th>Type</th>
<th>Last week</th>
<th>Weeks on list</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hotbar</td>
<td>09/23/10</td>
<td>Adware</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>Simda</td>
<td>06/13/11</td>
<td>Backdoor</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>VBlitecWV</td>
<td>05/01/12</td>
<td>MalwarePackage</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Kelihos/F</td>
<td>03/31/12</td>
<td>Backdoor</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>Beebone/DN</td>
<td>09/13/12</td>
<td>Downloader</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Beebone/DJ</td>
<td>08/31/12</td>
<td>Downloader</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Siret/P</td>
<td>12/04/11</td>
<td>Bot</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>Wobotus/HQ</td>
<td>09/10/12</td>
<td>Worm</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>Beebone/EA</td>
<td>09/21/12</td>
<td>Downloader</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>Allapple/A</td>
<td>12/05/10</td>
<td>Worm</td>
<td>1</td>
<td>7</td>
</tr>
</tbody>
</table>

Source: Kindsight Security Labs

**Index of cyber security**

Perceived risk

<table>
<thead>
<tr>
<th>Index value</th>
<th>Rate of change over previous month</th>
</tr>
</thead>
<tbody>
<tr>
<td>900</td>
<td></td>
</tr>
<tr>
<td>990</td>
<td></td>
</tr>
<tr>
<td>1,090</td>
<td>1.50</td>
</tr>
<tr>
<td>1,190</td>
<td>1.20</td>
</tr>
<tr>
<td>1,290</td>
<td>1.00</td>
</tr>
<tr>
<td>1,390</td>
<td>0.80</td>
</tr>
<tr>
<td>1,490</td>
<td>0.60</td>
</tr>
<tr>
<td>1,590</td>
<td>0.40</td>
</tr>
<tr>
<td>1,690</td>
<td>0.20</td>
</tr>
<tr>
<td>1,790</td>
<td>0.00</td>
</tr>
</tbody>
</table>

The index queries information security industry professionals monthly to gauge their perceived risk to the corporate, industrial and governmental information infrastructure from a spectrum of cyber security threats. A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite.

Source: ICS, www.cybersecurityindex.com

**Top 5 attacks used by U.S. hackers**

1. ZeroAccess trojan
2. Web-based exploit kits
3. Butterfly bot
4. Zeus trojan
5. Downloader trojan

**Top 5 attacks used by foreign hackers**

1. ZeroAccess trojan
2. Web-based exploit kits
3. Zeus trojan
4. Poison Ivy backdoor
5. Waledac trojan

There were 12,568,322 attacks in the United States last month, primarily originating from New York; Rochester, Minn.; Haines City, Fla.; Garden City, N.Y.; and Ft. Lauderdale, Fla. There were 18,717,015 foreign attacks last month, primarily originating from Mumbai, India; Bucharest, Romania; Rome; Moscow; and New Delhi.

Source: Dell SecureWorks
NEWS BRIEFS

The Canadian government unlocked $155 million in funding to bolster cyber security, just as the auditor general issued a negative report, which found that the government has failed to deliver on key promises made in 2001, when it said that it would partner with private sector organizations to protect critical national infrastructure (CNI). These partnerships have not been established in all sectors, and coverage is incomplete.

Some of the $155 million, announced in mid-October by Vic Toews, public safety minister, will go to the Canadian Cyber Incident Response Centre, but $12.4 million of the funds will be spent on bringing the Centre up to par. Launched seven years ago to collect and disseminate cyber threat information, it is still not operating on a 24/7 basis as originally intended, said the report, and many stakeholders still fail to understand its role.

Public Safety Canada and the U.S. Department of Homeland Security launched an action plan last month to back up a February 2011 border security partnership.

The two agencies outlined three goals in the action plan: enhanced cyber incident management collaboration among analysts, the two agencies will work together on briefing private sector organizations on cyber threats, and standardize protocols for sharing information, they said.

The Institute of Electrical and Electronics Engineers (IEEE) felt victim to a breach that exposed the usernames and passwords of about 100,000 members. IEEE, one of the world’s largest technology professional organizations, said an issue that arose in conjunction with its proxy server provider was to blame for the compromise. Radu Dragusin, a computer science researcher at the University of Copenhagen, found in Denmark, discovered the issue when he visited the IEEE’s FTP site and found the clear-text usernames and passwords of group members from around the world inside ZIP log files.

Team GhostShell, an anonymous hacktivist collective, claimed to expose more than 120,000 accounts and records gathered from servers at 100 top-rated universities domestically and abroad. According to the group, a laundry list of prestigious institutions were among the victims, including Princeton, Harvard and Johns Hopkins universities.

At minimum, the email addresses, passwords, IDs and names of students and faculty were found online. In a Pastebin message, Team GhostShell said the recent attacks were launched to bring attention to various grievances.

THE QUOTE

‘‘When the CEO asks how secure we are, I’m brutally honest.’’

—Phillip Ferraro, CISO of DR5 Technologies, on the fact that no organization can be 100 percent secure, but it’s how one responds to incidents that matters.

2 minutes on...
The resurgence of security IPOs

Me and my job
“I protect phones and computers to make lives better”

Skills in demand
Pros with database development training are needed

Jets in the news
Bank of America, Wells Fargo, PMC Bank, U.S. Bancorp and JPMorgan Chase were among the major banks affected by DDoS attacks.

Vaults, so passé
Major banks established website issues believed to be the target of DDoS attacks. A hacktivist group claimed responsibility for the incidents in protest of an inflammatory film “Innocence of Muslims.” The sites lagged or were intermittently down for customers, though affected banks were able to restore availability after a number of hours. None cited that any customer or bank information had been improperly accessed.

Debate
A White House order on cyber security would be a step in the right direction for safeguarding networks.

FOR
State-sponsored cyber attacks require a state-led response. President Obama’s planned executive order (E.O.) in response to the defeated U.S. Cybersecurity Act of 2012 (CSA) will allow federal agencies to propose new security standards for critical infrastructure industries. It will also create a council of federal agencies, led by the Department of Homeland Security, to report on cyber threats, many state-sponsored by China. The (failed cyber security) bill called for voluntary standardized security practices, liability protection, priority assistance and access to classified information for companies that control the nation’s critical infrastructure.

AGAINST
Critics argue the provisions are hallmarks of an intrusive government, that liability protection is inadequate, that non-participating companies would be penalized and that voluntary standards will stifle innovation. Such ideological myopia is both wrong and dangerous. The federal government must play a lead role in protecting the country and its institutions.

THE SC MAGAZINE POLL
Has your company website been the target of a DDoS attack recently?

46.88% No, it has never been a target.
31.25% Yes, in the last six months.
18.75% Yes, in the last year.

To take our latest weekly poll, visit www.scmagazine.com

THE STATS
50% increase in Q4 2012 over Q4 2011 in the total number of DDoS attacks

31% of 300 organizations polled in the U.S. and U.K. sustained at least one DDoS attack in the last 12 months (as of 3/12)

What is it?
A 0-day vulnerability that affects all supported versions of Internet Explorer and can be exploited to compromise a user’s system.

How does it work?
The vulnerability is caused by a use-after-free error when handling the “execCommand” method and can be exploited to dereference an already freed COM+1MEd object in memory to gain control of the program flow. This allows executing arbitrary code on a user’s system with the user’s privileges.

Should I be worried?
Users should show extreme caution when visiting untrusted web sites if their systems are not fully patched.

How can I prevent it?
Shortly after information on the O-Day was released, Microsoft confirmed the vulnerability via a security advisory and provided a temporary Fix It solution. On Sept. 21, Microsoft released an out-of-band security bulletin, MS12-063, which addressed the vulnerability, along with four other potential remote code execution bugs.

Source: Caroline Eason, chief security specialist, Secunia

The business of government is government, not private sector. Government safeguarding government assets is appropriate; however, declaring private sector part of the government “critical infrastructure” is a nebulous definition at best. Collaboration among partners is laudable given an equal footing, but when one partner holds authority or provides direction to other partners, the collaborative facade evaporates. Information sharing is desirable among teammates; dialogue is bi-directional. Open communication is key.

Cyber security needs responsible, accountable, technically savvy individuals to drive vision and create the way forward, not politicians who drive meaningless mandates. In the ever-changing landscape where cyber space meets business, the private sector in America still means businesses are accountable to shareholders, employees, and customers. Who knows business best? Who protects our assets? He who owns a thing, controls the thing. That’s how democracy works.
The resurgence of security IPOs

A fter the economic crash in 2008, the public market has slowly begun to improve, and what seemed like an utter drying up of capital is now beginning to dampen. While Face book’s initial public offering (IPO) was a bit of a black eye for the technology industry, the security software market could be making up for it. LifeLock, Qualys, Proofpoint, Splunk and Palo Alto Networks are a handful of prominent security firms that have gone public this year—and have seen success. According to Thomson Reuters, 60 percent of the venture-backed IPOs issued in the third quarter of this year are IT related. Of that bunch, the largest IPO of the quarter came from Santa Clara, Calif.-based firewall vendor Palo Alto Networks. After releasing its IPO shares on July 19, it saw a 27 percent increase by day’s end. As of Oct. 10, the stock is up 47 percent from its IPO. Qualys, a Redwood, Calif.-based cloud security company, saw similar success when it released its IPO on the Nasdaq stock exchange in September, debuting its offering at $12 a share and closing the day with an 18.5 percent gain. Prices have increased 13 percent from its IPO as of Oct. 10.

The number of software security IPOs is indicative of the high demand for innovative technology, said Gary Steele, CEO at Proofpoint, a Sunnyvale, Calif.-based company that offers cloud-based security solutions and went public in April. However, Steele said, while there are some perks in having access to additional capital, there are attendant risks involved with going public.

“You have to believe that you can sustain your business over a long period of time, and, if you don’t believe that, the risks are very high,” he said.

The trend of industry giants, like Symantec and McAfee, buying up the smaller specialized companies seems to be deviating, said Dov Yoran, CEO at ThreatGRID, a New York-based strategy and business advisory firm in the information security market. Though acquisitions are still prevalent, he believes that the innovation from smaller software security companies are upping their price tags. That may not be as attractive to security titans deciding whether to make the move and match them up.

“Maybe it’s a trend that’s going to evolve and we’re going to see more companies heat up with the security market in general and we’ll see more that are going to take the option of going public rather than getting acquired,” Yoran said. — Marcus Colon

JOBS MARKET
Me and my job

Grant Sobb proactive investigations program manager for Intel IT

Why did you get into IT security?
I followed in my father’s footsteps. He worked in IT security for a decade before I started.

How do you describe your job to average people?
I work in computer security and we keep an eye on the data that is used to build our company’s products. We have to protect it so that phones and computers keep getting better and in the process make people’s lives better.

What was one of your biggest challenges?
The biggest career challenge I faced is turning around the convention in my field that you were either technical security or security management. I’ve been successful at both, and we need more people who can wear both hats. I’ve also found valuable perspective in seeing both the technical and management sides of an issue.

What keeps you up at night?
I worry that information security organizations are not changing fast enough in a changing world. So many have been “fighting fires” for so long they may have not learned new “fire prevention” techniques along the way.

It takes time and resources to be proactive, which are always in short supply.

Of what are you most proud?
I worked at a company which supported my efforts to develop a new approach to securing data and then supported my desire to release it as free software to help the rest of the world with the same task. I believe there is a lot of benefit in an IT department sharing a success with other IT departments worldwide.

For what would you use a magic IT security wand?
I would want to equip all information security incident responders with the best tools to quickly and efficiently handle incidents. I know there are people who are kept away from their families doing this work, and I want to get them home sooner.
Building a trustworthy mobility program

Michael Scovetta, director of advanced technology at a large media/entertainment company

As we approach the end of 2012, nearly all large enterprises have at least partially adopted smartphones and tablets for business purposes. Nearly three-quarters of them have started to implement bring-your-own-device (BYOD) programs. As device adoption continues to grow, the importance of implementing a secure enterprise mobility program cannot be understated. There are many aspects that should be included in a successful program: A mobile device management (MDM) solution should be implemented to protect enterprise data from loss via untrusted devices. As well, a process for developing and deploying secure mobile applications must be put in place.

Over the past few years, MDM solutions have gained significant traction in the enterprise, and should now be considered critical components of an enterprise security program. Choosing the right MDM solution for your organization can be difficult, especially at the frenetic pace of the mobile market.

First, ensure that the solution provider has a track record of supporting a range of current mobile devices, even if you only plan to support specific platforms right now. As new devices come on to the market, you want to be sure that the solution will grow with your needs.

Next, base your MDM configuration on existing security policies, especially for data encryption, password strength and remote wiping. As well, consider using a transparent, on-demand VPN. Since many users will be accessing mobile applications from untrusted wireless locations, the use of a VPN to secure traffic out of the device can serve as a stop-gap against vulnerable applications.

This can be a difficult time to choose a mobile application development architecture — with standards like HTML5 quickly evolving and device capabilities and form factors advancing just as rapidly. Regardless of the architecture you choose to implement, it’s important to ensure that enterprise data remains protected on mobile devices.

It’s imperative to include mobile applications and API endpoints in existing vulnerability management processes. Remember that mobile applications can be affected by most of the same vulnerabilities as traditional desktop and web applications.

The enterprise mobility space has expanded enormously over the past few years and shows no signs of stopping. Threats to enterprise data continue to increase, and protection of that data is paramount. The use of a comprehensive MDM solution and a secure mobile development program can significantly reduce the risk inherent in these powerful devices to help your organization to realize their benefits.

Got something to say?

From the online mailbag
In response to a September news story, Wyndham Hotels challenges FTC security suit over breaches:
Hotels small and large are to a large extent totally floating the Payment Card Industry Data Security Standard and I expect the card brands will not want to come down on them too hard, but it has to happen soon.
Jon Bays
Industry standard best practices is an oxymoron.
There is industry best practices and industry standard practice. If there is no compliance framework, then a subjective risk management procedure could be seen as reasonable. Proving gross negligence isn’t simple.
Sebastian
In response to a feature story in September, Why can’t we be friends?
Mistitled leading...When I first read the title, I thought this article was going to be about merging accountabilities and management for physical and cyber security, and I was ready to jump in with, “Been there, done that, it doesn’t work...” As it turns out, this is really just about IT (not cyber security) doing a better job supporting the physical security function of the organization. It’s only the final paragraph that quotes Terry Neely (CTO, RedCloud) on the need for converging the physical and cyber security organizations, but there is NOT supporting evidence. I’ll keep mine separate, thank you. We’ve had a lot fewer successful attacks since we split them apart, and still successfully integrated our physical and logical access controls and HR system, deployed IP-based video surveillance, integrated our business processes and policies, and much more.

Letters

Letters

There are safer ways to work together

Axway DropZone™ keeps file sharing & collaboration safe-for-work

For a free 30-day trial, visit us online at axwaysecurity.com or call 855-627-1258

The opinions expressed in these letters are not necessarily those of SC Magazine.

To further protect enterprise data, Michael Scovetta advises that administrators maintain a comprehensive security threat model for the use of mobile devices in the enterprise.

> Safeguarding data
> Get policies in place
> Automate processes
> Layer protections

30 seconds on...

Send your comments, praise or criticisms to scfeedbackUS@haymarketmedia.com. We reserve the right to edit letters.

Michael Scovetta advises that administrators maintain a comprehensive security threat model for the use of mobile devices in the enterprise.
One desktop should not be able to assault the entire network from within..."
Information security is a challenge across industries, but arguably no vertical has more personally identifiable information to protect than government. In fact, government agencies typically are swimming in the confidential data of the large numbers of taxpayers who they serve. But that’s where a delicate balancing act comes into play, because, often, government workers’ jobs center on interacting with the public and responding to their requests for information.

“That’s why state government is here, to serve the people of the state,” says Theresa Masse, CISO of the state of Oregon. “We want to be helpful. We’re here because of their tax dollars. We want to make sure we’re giving the highest level of service that we can. [So] people tend to be helpful. [But] it’s important to realize that when it comes to confidential information, we have to be careful what we’re giving out and who we’re giving it to. We have a responsibility to protect that information.”

Masse, 59, who has served as Oregon’s security chief for the past seven years, says that because government employees tend to share personal information with citizens more than most organizations do, the threat of an insider-caused breach is ever-present. And with 58,000 employees operating across 110 agencies, boards and commissions, it’s easy to understand why Masse views the Beaver State’s workforce as the first – and often, last – line of defense against breaches.

And the threat doesn’t merely reside in Oregon state employees’ handling of sensitive information — such as data related to unemployment or welfare benefits — but also in the possibility that their actions may open the door to an external adversary.

It’s not that far-fetched a scenario. In October, hackers raided the bank account for the city of Burlington, Vt., making off with $400,000 after city computers were compromised to steal login credentials. The heist hijacked the direct deposit account information for a large number of municipal employees, and the perpetrators’ identities remain unknown.

As such, it takes just one hacked endpoint for a financial disaster to be set in motion. And with attacks becoming more sophisticated and so-called disruptive technologies, like social media, mobile devices and cloud computing, becoming commonplace, attacks that succeed via the mistake of an employee are more of a reality than ever.

“Phishing and social networking have enabled external folks internal access through employee accounts,” Masse says. “This often is more difficult to detect, as employees have legitimate access, frequently to very confidential information, as part of their job functions. So whether employees are misbehaving or their accounts are compromised by an external source, state information is very much at risk.”

Although according to breach repositories, data-loss incidents caused by external adversaries traditionally have trumped those committed by insiders, studies show that insider-enabled events often are underreported — and can lead to significant brand and reputational harm. Carnegie Mellon University in Pittsburgh, which earlier this year studied 80 cases of insider fraud in the financial services industry, found that “low-and-slow” acts of insider fraud are costing organizations an average of $382,000. The study, funded by the U.S. Department of Homeland Security, turned up some potentially surprising tidbits, including that managers and accountants...
because you brought something for-

Think of it as a version of the Depart-

to detect and potentially can compromise
or their agency’s security mechanisms,
Masse says. “Presumably, they have
are causing the most damage, and that
User education

In an effort to avoid this type of fate, the state of Oregon has focused its pro-
tion on defining data, logging
ents and controlling access. But Masse
also has one other trick up her sleeve to get
employees more security minded. Think of it as a version of the Depart-
ment of Homeland Security’s “If you see something, say something,” campaign, but applied for information security.

“You’re not going to be penalized because you brought something for-
ward,” she says. “It’s water under the bridge. Accidents happen. Life happens. That’s OK. Let someone know so appropriate action can be taken. It may be nothing, but we’d rather investi-
gate than have it simmer.”

Is training worth it?
Most security experts believe compre-
hensive policies and robust user aware-
ness training are critical underpinnings
for any organization’s security program. When it comes to organizations sus-
aining malware infections, the source of the attack is often an unwitting user
who clicks on an attachment or link that they shouldn’t. As such, the theory goes, if the user were properly trained to spot
attempted network intrusions, many of
those today’s most devastating breaches could be stymied.

Many organizations have taken that to mean they must invest in security awareness programs, which vary in shape and size, but commonly take the form of
users passing an annual exam to validate
that they aren’t going to click on that

researcher Adam Shostack, who contend-
ed that awareness programs should only
be written off if organizations determine
they’re not worth the investment. To
accomplish that, he challenged companies to develop more reliable risk metrics.

“Opinions, including mine, Dave’s and yours, just aren’t that good,” in the face of data,” Shostack wrote. “If you’re out-
raged by Dave’s claims, prove him wrong. If you’re outraged by the need to spend money on (training for) social engineer-
ing, prove it’s a waste.”

Mark Johnson, chairman of the U.K.-based Risk Man-
gement Group, a consulting firm, sides with the belief that
training employees probably isn’t worth it. Considering the emergence of BYOD, social
media and cloud, Johnson would instead like to see end
user organizations demand
more of their providers.

“There’s a tendency to blame employ-
ees, as if they’re somehow at fault,” he says. “What we’re looking at is a de-
centralization of (mobile) devices. Employees are deciding what to install, which network to use. They’re acting as if they’re system administrators, and most of them haven’t been trained for that. I think the responsibility of telecom
operators and manufacturers of devices
is to put strength in the hands of users. It would seem that more could be done,
given our dependency (on their services and offerings).”

And the problem will only grow, he calculates, considering that risk is a function of the number of devices, vulnerabili-
ties and malware samples that are present, all of which are growing at

Information Systems Security Laboratory at the college in Anaheim, CA.

Billed as a first-of-its kind effort, the for-
profit center will offer training, product testing and outreach specifically
gear for IT workers – not security
professionals who are employed at small and midsize businesses in Iowa and
across the Midwest.

“They play a critical role in the way the organization operates,” he says. “They’re not the ones who are often in charge of a lot
of the infrastructure. If they don’t have a good handle on security, they may see things they may not know they’re seeing. IT staff needs to be aware of threats.”

“IT’s not going to be able to go out and buy top-of-the-line (products).”

Shoestring security
In Oregon, like any government, espe-
cially one operating in a recession, bud-
get dollars for security – and across the board for that matter – are at a premium. Stuck in a spending quagmire for several years, Oregon has faced job losses and has been forced to institute mandatory
employee furloughs, says Masse, who oversees the state’s enterprise security office, which is responsible for develop-
ing policies, standards and guidelines for all of Oregon’s government agencies.

Masse admits that an employee base of nearly 60,000 presents an unexplored exploitable threat. It is now
in training workers, especially on the fundamentals – like not sharing one’s
password and not clicking on suspi-
cious links or attachments. And even basic enterprise direc-
tives that each agency must have an information security training program in place, Masse’s office also has formed a 25-person information security council, which meets on a monthly basis to discuss critical
issues. The state also leans on a num-
ber of no-cost initiatives, such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), which provides complimentary materials, such as literature and webcasts, that can be shared with all of the state’s agencies. In addition, Oregon has participated in a federally run two-day exercise known as Cyber Storm, which forced key personnel in various state depart-
ments to engage in and respond to simulated cyber incidents. The state also has established a Federal Tax Information Committee, which includes members from various departments that handle highly confidential tax data –
such as the Department of Revenue and the Department of Human Services.

Ultimately, educating trusted insid-
ers is just one tool in any organization’s security arsenal, Masse says. And even if it would be prudent to expand on best practices, there’s no way to guarantee that there won’t be a bad apple among the bunch. That’s why the only rational
tactic to take is to consider and present the best business practices, and work

22 SC • November 2012 • www.scmagazine.com www.scmagazine.com • November 2012 • SC 23
Voluntary guidelines for reporting data

a provincial level.

given companies a total ‘get out of jail

the opposite, he warns. “It’s actually

data breach notification rule, is almost

ernment legislation that offers a federal

area, he doesn’t think the nation is going

of ongoing government legislation in this

tions report data breaches. But in spite

requirement that would make organiza

of Canada’s Public Interest Advocacy

the same time. The executive director

In fact,

ommunications reports.

among its existing duties. But with the

PIAC wants a strong federal

Centre (PIAC) wants a strong federal

extent to which they are following the

the government.

the complexity of the rules.

The government introduced a bill.

the government.

Finally, in 2012, a political will
t is revised.

But sadly for privacy advocates, Alberta

the company will say ‘So what? Have a

show that it’s time

Newly released government

figures show that it’s time

for a nationally enforced data breach reporting mandate, reports

Danny Bradbury.

John Lawford is not a happy man.

You can hear it in his voice, which

is both resigned and resentful at

the same time. The executive director

of Canada’s Public Interest Advocacy

Centre (PIAC) wants a strong federal

requirement that would make organiza-

tions report data breaches. But in spite

of ongoing government legislation in this

area, he doesn’t think the nation is going
to get one.

In fact, Bill C-12, the forthcoming go-

vernment legislation that offers a federal

data breach notification rule, is almost

the opposite, he warns. “It’s actually
given companies a total ‘get out of jail

free’ card.”

Most would agree that it is important
to notify the public when an organiza-
tion has experienced a data breach that
places personal information at risk, but

it has taken a long time for most Canadian

governments to realize this, at a federal or

a provincial level.

Today, Jennifer Stoddart, the fed-

eral privacy commissioner, has a set of

voluntary guidelines for reporting data
breaches. These guidelines don’t mandate

the reporting of data breaches to the commissioner, but rather

encourage” it.

These best practices have produced

mixed results. The commissioner’s latest

annual report shows that the number of
breaches reported has varied substan-
tially, dropping from 65 in 2008, to 58
and then 44 in subsequent years, before

picking up to 64 again in 2011.

The softness of voluntary guidelines is

one reason for the push toward manda-

tory data breach notification. The impetus

came from the first five-year review of

Canada’s Personal Information Protection

and Electronic Documents Act (PIPEDA)
in 2007, says Tim Banks, a partner and

expert on data governance law at Fraser

Milner Casgrain LLP in Toronto. “But it
took the government until May 2010 to
do anything about the recommendations from

that review.”

The government introduced a bill,

including a mandatory data breach

notification clause, which died after

parliament was dissolved for the election

in March 2011.

Bill C-12 is another attempt to bring

forward this

data breach notification,” says

Banks. The bill, which was

introduced in September 2011, has been

through its first reading, but has stalled

since. “It doesn’t seem to be a priority for

the government,” he says. “It’s hard to

see what the commitment is to bring this

into force.”

Lawford is unimpressed by the bill.

It gives excessive discretion to organiza-
tions to determine whether a data breach

will harm consumers, he said in a Janu-

ary 2012 report.

“The idea is there, but the test is

wrong,” he says. There are two stages in
determining whether the public should

be notified in the event of a data breach.
The first is the company deciding itself

whether it should report an incident to

the privacy commissioner. The second is

the commissioner deciding whether the

breach is serious enough to be reported to

individuals affected.

PIAC worries that the first test is pro-
hibitive. Section 10(1)(2) of the bill uses

three factors to determine whether a

breach should be reported to the privacy

commissioner. One of them is “an assess-

ment by the organization that the cause

of the breach or a pattern of breaches

indicates a systemic problem.”

This effectively condemns a company
to negligence if it reports a breach to the

commissioner, says Lawford. “Anyone

who reports to the privacy commissioner
effectively opens up their company to

being sued,” he says.

Because of the way the law is writ-
ten, companies could attempt to define

a data breach as non-systemic to avoid

litigation, says PIAC’s report. Moreover,

because the onus to report is on the

compromised organization, the com-

missioner would be hard-pressed to find

otherwise unless it had the authority and

resources to conduct an in-depth audit

of the organization’s internal systems.

The other big problem lies with the

second stage, Lawford warns. Under Bill

C-12, the privacy commissioner formally

gets to decide whether to notify individ-

uals, but doesn’t have enough knowledge
to make that decision. The decision

turns on whether the data breach poses

a “real risk of significant harm” to

individuals. “Real risk” relies on the

breached company’s own interpreta-

tion of how sensitive the compromised

personal information is, and how likely it

is to be misused. PIAC believes that the

privacy commissioner has no formal role

in making these determinations under

the proposed legislation.

“If the current C12 were to become

law as proposed, private sector organiza-

tions would be obligated to report data

breaches to our office, but the legisla-

tion lacks the teeth it would need to be
effective,” a representative for the federal

privacy commissioner’s office says. “For

example, regarding organizations that

refused to comply, our office would face

the prospect of building an uncooperative

compny to court to have them notify us,

let alone their customers, upon a breach.”

PIAC recommended that all data

breaches be reported to the privacy

commissioner within 48 hours, on pain

of monetary penalties. It should be up to

the privacy commissioner to decide on

customer notification. She should also

have the power to audit data protection

measures, particularly around breach

notification procedures, and she should

devote a whole division to this topic,

with a breach advisory board, PIAC said.

It also called for an object test for “real

risk of significant harm”.

This is all a far cry from Alberta,

which is the only province in British

Columbia to introduce mandatory data

breach legislation. In 2009, it reviewed

its Personal Information Protection Act

and decided that there was a need to

force organizations to notify the com-

missioner of information losses if they

constituted “a real risk of significant

harm”, letting the commissioner decide

whether to notify individuals.

There are several key differences

here. The first is that the test for “real

and significant harm” is simpler than is

proposed by C-12. It rests on whether a

reasonable person would consider the

information loss to present real and sig-

nificant harm to an individual. It doesn’t

call for a company to admit systemic

failure in its privacy controls.

The other difference is that unlike the

federal privacy commissioner, the Alberta

privacy commissioner has order-making

power. It can fine an organization up
to $100,000 for not reporting a privacy

breach as non-systemic to avoid

notifying of affected individuals. Up
to 420,000 Albertans were affected by a

single breach, the commissioner found.

Clearly, mandatory breach notifica-

tion has an effect when backed up by a

commissioner capable of making orders.

But sadly for privacy advocates, Alberta

is the only province to have amended its

privacy act for mandatory notification.

R.C.’s Privacy Commissioner Elis-

beth Denham has said that mandatory

notification should be made law, but this

has not happened. Some provinces, such

as Ontario, have strong specific legisla-

tion, which forces mandatory reporting

requirements under its Personal Health

Information Protection Act.

Comparing the number of breaches

reported over two years in Alberta (151)

with the breaches reported country-wide

under voluntary federal guidelines during

roughly the same period (108), backs up

privacy advocates’ call for manda-
tory reporting. But the impetus doesn’t

seem to be there, and the iron, once hot

to strike, is cooling. In her latest annual

report, the federal privacy commissioner

pointed out that the provisions in C-12

are already out of date, as they were based

on recommendations made in 2006.

Perhaps things will change in the

five-year Personal Information Protection

and Electronic Documents Act (PIPEDA)

review, which was meant to happen in

2011, but which has still not been under-

taken. Perhaps at that time, the federal

privacy commissioner will finally gain some

order-making capability, and the provi-

sions in Bill C-12 will be updated.

“Bill C-12 doesn’t seem to be a

priority for the government.”

—Tim Banks, partner, Fraser Milner Casgrain LLP
Stuxnet was a game changer, but control systems that run the nation’s infrastructure are still at risk, reports Deb Radcliff.

For more than 10 years, they saw it coming: SCADA (supervisory control data acquisition) systems managing critical infrastructures would be targeted by cyber terrorists, activists and government-sponsored agents. The results would be catastrophic.

Working groups formed under the North American Electric Reliability Council, the International Society for Automation (ISA), ASIS (American Society of Industrial Security), and Information Sharing and Analysis Centers (ISACs). System operators needed to be educated about cyber risks, best practices needed to be formed and standards needed to be set.

Then, June 2010 came around and news of the Stuxnet worm broke. “Stuxnet immediately became a major concern in our infrastructure meetings,” says Mark Schreiber, vice chair of the critical infrastructure working group for the ASIS, and security system design engineering specialist at Fluor, a Irving, Texas-based company that provides project management to clients around the world.

Dale Peterson, president of Digital Bond, speaking at the company’s S4 conference, where the best SCADA hackers and researchers share the latest in exploit code.

“We have a clear understanding that control systems run on computers and are susceptible to threats, he says. Now they need to fully understand the consequences of system failure or malicious manipulation.

“Thanks to Stuxnet, people understand that control systems run on computers and are vulnerable to attacks,” says Eric Cosman, vice president of Digital Bond, a Foxborough, Mass.-based provider of automation system management. “It’s a huge challenge for these organizations, especially since many of these devices don’t even have logging capability.”

authentication is not practical, one has to keep its control networks segmented, monitor what one can, and deploy controls all the way to the substations and the endpoints plugging into the control networks, says James Culline, product line manager for HP Enterprise Security.

“When it comes to SCADA and other control systems, the key priorities are reliability and uptime,” he says. “So SCADA operators need to look at their own systems, set their security policies and implement controls that are specific to their networks.”
While talking to some customers, Dan Holden, director of ASERT (Arbor Security Engineering and Response Team), a division of Chelmsford, Mass.-based Arbor Networks, noticed a "fundamental" shift in how they were looking at security.

These organizations, Holden found, weren’t planning out projects to deploy anti-virus, firewall or intrusion prevention systems throughout the enterprise. Rather, they had projects addressing specific problems, such as botnets, distributed denial-of-service attacks (DDoS) and advanced persistent threats (APTs).

"They weren’t planning out projects to deploy the best everything in the market," Holden says. "They were solving these problems," and were not asking what products they should be buying. The realization was an "ah ha" moment for him. The threat landscape was driving the conversation on how to defend the network, which is a departure from the past, when administrators typically first deployed the security technology and then figured out how to block the attacks, Holden says.

The average network has grown exponentially over the past few years – with many people having more than one internet-connected device and spending more time online for both work and personal use. Having insight into what is entering and leaving the network is critical, and the ability to block malicious traffic from coming in is paramount. But specialized systems and advanced network security technologies have hit the market in recent years, there is no reason for organizations to abandon mainstay solutions, such as intrusion prevention systems, experts say.

“Defense-in-depth doesn’t mean buy the best everything in the market,” Holden says. The integration has “positive implications” for performance and reliability, according to Al-Abdulla.

Traditionally, organizations bought IPS and deployed the technology as the first line of defense outside the network perimeter and the firewall, Stella, CTO of Network Box, a Houston-based computer security systems provider. All traffic first had to pass through the IPS and then the firewall, before reaching individual systems inside the network. The IPS was designed to be fast and lightweight in order to scan, identify and block malicious packets without slowing down network performance, Stella says.

And, as the network expands and evolves, basic security measures should remain the same. “I still have a strong door to keep people out [of my house], even though I have an alarm system and a camera,” Stella says. The fact that IPS is a decade old doesn’t mean it’s still not useful, says Daniel Ayoub, manager of product marketing at Dell SonicWALL, a Round Rock, Texas-based provider of network security. Firewalls are 25 years old and still considered a critical component of the network infrastructure, he says. And, IPS is just as ubiquitous – with Ayoub estimating that nearly 98 percent of organizations have deployed an IPS in some form or another.

If the organization doesn’t already have an IPS deployed, Network Box’s Stella recommends investing in newer technology and security protections. However, for organizations where the technology is already running, he doesn’t see any reason to “toss it.”

Even if the IT department never looks at the logs and alerts within the IPS, simply having technology that blocks “known evil” provides a “reasonable level of protection” against ubiquitous threats, such as propagating worms, says Sadik Al-Abdulla, senior manager of the security practice at CDW, a Vernon Hills, Ill.-based provider of technology products and services. While IPS won’t be able to block attacks exploiting zero-day vulnerabilities or thwart a skilled adversary using sophisticated tactics, it should “prevent 99 percent of push-button or automated attacks,” Al-Abdulla says.

That’s not to say IPS technology hasn’t evolved and matured over the years. While the solution originally relied on signature databases to identify bad packets, most modern systems have added reputation analysis to discern when requests are coming from known malicious sites and to detect anomalies in network traffic.

The evergreen IPS has evolved, but some experts dispute whether new features are enough for today’s attacks, reports Fahmida Y. Rashid.

The integration has “positive implications” for performance and reliability, making deployment simple and more cost-effective, agrees Al-Abdulla. Stella goes a little further, saying that IPS should no longer be used as a standalone technology, and instead should be tightly integrated with the firewall. In today’s threats, says Tyler Carter, head of product marketing at McAfee, a Santa Clara, Calif.-based security software company. While baseline scanning using signatures is important, using reputation scanning to flag “bad neighborhoods” and identify suspicious behaviors is now part of the IPS arsenal, he says.

For example, if a machine on the network, usually used as a web server and email client, suddenly started surfing the web, that change in behavior is a red flag, Carter says. A file that claims to be a PDF file, but doesn’t seem to behave like one, would also be flagged.

Convergence

Customers often rely on default policies despite the fact that the modern IPS can do much more than older systems, Carter says. Most organizations don’t have the time to manage these systems. They generally just configure the appliance to use the default policy and stick it on the network, he says.

If vendors improve the quality of the default protection, then the customer gets a better level of protection out of the box, Carter says. There’s also a convergence happening – with IPS being integrated into other networking products. Holden says IPS capabilities are now found in routers, switches, firewalls and unified threat management systems, among others.

The integration has “positive implications” for performance and reliability, making deployment simple and more cost-effective, agrees Al-Abdulla.

“I always have a strong door to keep people out of my house, even though I have an alarm system and a camera,” Stella says. The fact that IPS is a decade old doesn’t mean it’s still not useful, says Daniel Ayoub, manager of product marketing at Dell SonicWALL, a Round Rock, Texas-based provider of network security.
Network protection

IDS will fall by the wayside in the next three to five years.”

—Dan Holden, director of ASERT

that scenario, the IPS side of the system would identify rogue network packets, and the firewall side would drop the connection and block further attempts.

But, integrating the IPS with other networking components doesn’t mean putting them inside the same box. In fact, it’s better to focus on an integrated system where different components work together, but are separate entities, says Carter. There is a push to consolidate, but when a single appliance has to handle anti-virus, SSL encryption and date, but when a single appliance has to handle anti-virus, SSL encryption and other tasks alongside basic firewalling, performance is diminished greatly due to resource constraints.

Yet, security technology can’t operate in isolation, as the endpoint has to know what’s happening in the network, and the network has to know what’s happening in the endpoint. Carter says. The challenge is to be available and effective without getting in the way of the network.

Holden of Arbor Networks agrees that even though IPS is an evergreen technology, there are certain areas where it is no longer useful. As attack methods and type of threats hitting the networks evolve, the effectiveness of an IPS has dropped. In the past, most network traffic was protocol-based, which IPS was good at blocking, but now much of the traffic going in and out of the network is content-based, which IPS has difficulty figuring out, Holden says. Attacks using obfuscated JavaScript to hide their activities is a nail in the coffin for IPS, he says.

In addition, an IPS gives administrators visibility into network traffic; it struggles with web application traffic, as it cannot differentiate between legitimate application traffic and a malformed request designed to attack, says Rob Rachwald, director of security at Redwood Shores, Calif.-based data security company Imperva. Organizations with web applications need to close the gap with web application firewalls (see sidebar below). While the IPS scrutinizes traffic against signatures and anomalies, the WAF determines the behavior and logic of what is requested and received by the application, Rachwald says.

While the IPS is still considered viable, its sister, the intrusion detection system (IDS), hasn’t fared as well. IDS is reactive as it is just detecting what is malicious, but today’s administrators want to take active steps to protect the network, such as blocking threats and other suspicious activities. Holden predicts IDS will “fall by the wayside” in the next three to five years.

It doesn’t do anything inside the LAN or outside to prevent intrusions into the network, Network Box’s Stella says. Its alerts and detection capabilities are useful after a data breach, but by the time it even sees the traffic, the network has already been compromised, Stella says.

In the past, administrators could look at the IDS logs to find breaches, but now there is too much network data being generated for that to be a worthy task, Holden says.

“The assumption is that someone is poring over pages and pages, screens and screens of alerts to make sense of them,” Stella says, adding the customer “derives zero value” from an IDS.

Many Network Box customers continue to deploy standalone IDS, simply because the auditors tell them that they have to, Stella says, adding, “Frankly, neither they nor I understand why.”

WAF: With a side of PCI

Web application firewalls (WAF) have an odd reputation within the security industry, as there are purists who think it is “immoral” to deploy the technology because WAF doesn’t actually fix issues in the application code, says Rob Rachwald, director of security at Imperva. Rachwald calls the sentiment silly, claiming that organizations should treat WAF as the first and last line of defense.

Considering the increase in web-based attacks, especially those using SQL injection, to breach the network by exploiting application vulnerabilities, protecting the web application is a critical security component, Rachwald says. Of all the incidents in 2011 where data was actually breached, 76 percent were web-based attacks, according to the “2012 Data Breach Investigations Report,” released by Verizon Business.

The defender dilemma has the defenders scrambling to know all the vulnerabilities in the application, Rachwald says, noting that attackers need to know just one. WAF is the best option to protect the application from attackers, Rachwald says.

However, in order to be PCI-compliant, organizations that process any kind of payment data must ensure that web-facing applications are protected against known attacks. PCI requirement 6.6 spells it out, mandating that organizations either install an application layer firewall or have all custom application code periodically reviewed by auditors specializing in application security.

But, proper code review programs take a long time to implement and it is sometimes difficult for smaller organizations to overhaul existing infrastructure, says Rachwald. Many organizations may not even have access to the original source code, making application scanning difficult. For many of them, not having to muck around in the source code is an attractive option, Rachwald says. – FR

Third-party access

The cloud presents new challenges in protecting data, such as who is responsible for implementations, Stephen Lawton reports.
in taxpayers dollars will be saved by 2020 by leveraging such technologies as Google Apps for Government. – U.S. Dept. of the Interior

Privileged users – those who have access to data based on their credentials – can pose a legitimate weakness, regardless if the users work for the owner of the data, a service provider or a business partner, he says. One important key to protecting confidential data, regardless of whether it resides locally or in the cloud, is provisioning, Papageorge says. The more users who have access to confidential data, the greater the vulnerability footprint.

Restricting access to a need-to-know basis can limit potential issues, Papageorge adds. Further, companies need to put in place countermeasures and controls, such as policies for security, administration, physical access to servers and the technologies used to run and protect the systems themselves.

Monitoring usage, access and activities are critical to ensure that corporate policies are followed, he says. When defending against an external attacker, the company will have a number of physical and logical protections in place – everything from the firewalls to the premises to login and password controls on users. However, he says, with an internal threat, many of those defenses are, by definition, bypassed, be the attacker malicious, such as an employee who is stealing data from the company, or the employee who accidentally leaves an exposure by leaving a VPN open or an unattended machine logged on.

Unwitting mistakes Insider threats need not be malicious in order to be destructive. Corporate IT departments do not give up management control of their own internal applications and data to the cloud. “You have more responsibility,” Papageorge says. “The probability of errors is higher.” Companies that outsource computing resources, including applications or even a full infrastructure, must not relinquish their management or monitoring responsibilities, he says. Doing so will increase the possibility of errors and attacks. Large corporations likely are aware of this need already, as they tend to have professional IT and security staffs that understand risk management. A small or midsize business (SMB), however, should get advice from security professionals before turning over any responsibilities to a third party.

“Advice is not expensive,” Papageorge says, adding that the cost of a data leak could be far greater than the price a company would pay for professional security consulting.

This possibility is neatly illustrated by the case of Mat Honan, a former contributing editor for Wired magazine, who in August was the victim of a real-based attack. The invasion was caused, in part, by a help-desk employee who unwittingly gave the attacker access to Honan’s private cloud account. The attacker allegedly compromised his Gmail, Twitter, Amazon and Apple iCloud accounts, ultimately resulting in the loss of all data from all of the devices. As part of the attack, the hacker gained access to Honan’s credentials by duping a rep at Apple’s online help center into providing Honan’s personal information, saying that he needed assistance accessing the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.

One solution to vulnerabilities such as this one may be mitigated by what Forrester Research, in its report, “The Forrester Wave: Enterprise Cloud Identity and Access Management, Q3 2012,” defines as the “smart cloudward turning IAM [identity and access management].” The report projects the segment emerging into an “explicit business enabler rather than a mere cost center and putting more focus on federated identity administration versus front-door authentication and access control into remote apps.”

To address these vulnerabilities, a contributor to SC Magazine was able to access a rep at Apple’s online help center, claiming that he needed help setting up an iCloud account for his friend. After gaining access to the iCloud user name and password, he was able to access the account. To gain access, he then contacted Apple accounts, who unwittingly gave the attacker access to the account.
Mobility is empowering individuals and, arguably, boosting productivity. But this harmonious picture is balanced by another vision of mobility as an unchained malady — multiplying the threat environment and thus making securing the enterprise even harder to achieve.

More and more end-users expect and demand to use their own mobile devices for work-related tasks. For many IT security pros, this brings your-own-device (BYOD) megatrend means the creation of gaping data security holes. It is a reality that won’t go away, but also one that is spawning an array of creative responses as companies devise best practices and implement new, countervaluing technologies.

“Organizations and IT can no longer deny corporate access to personal devices,” says Melissa Siemens, director of marketing for Santa Clara, Calif.-based McAfee’s software-as-a-service business. “So IT needs to determine how to not only secure these devices, but also the data and the applications on the device.” And, she adds, IT must be able to manage and report on those devices, and maintain compliance by understanding what data is on them.

Indeed, at MasterCard Worldwide, Edgar Aguilar, group executive of infrastructure and operations services, says information security has become the main driver for his organization’s BYOD design considerations. “As such, we have in place very tight engineering parameters, system controls and internal processes to protect the corporate information and our users worldwide,” he says.

The advent of BYOD introduces additional threats to the corporate security landscape, says Tyler Shields, senior security researcher at Veracode, a Burlington, Mass.-based provider of cloud-based risk assessment. “Some of the security problems exacerbated by BYOD, he says, include application-level security — particularly flaws and malicious code within downloaded applications, the loss of a device, device compromise and the disclosure of sensitive data via a personally owned device.

“Depending on the risk tolerance of the organization, some firms have created policies that enforce a much higher level of security than other companies that might have a more open and risk-accepting culture,” says Shields. However, he says, the majority of organizations are responding to BYOD with a mix of mobile device management (MDM), enterprise application stores, anti-virus and application scanning services.

“How much of the corporate security budget is being applied to these solutions is dependent on the risk-to-reward equation of allowing BYOD in the first place,” he says.

The majority of enterprises in the United States have or are planning to implement some kind of BYOD strategy, says Puneesh Chaudhry, co-founder and CEO of Copius, a Marlborough, Mass.-based provider of mobile collaboration solutions. In fact, by 2015, the “IDC Worldwide Business Use Smartphone 2011–2015 Forecast and Analysis” predicts that the majority of business-use smartphones worldwide will be employee liable (55 percent) versus corporate liable (45 percent).

“The reason this trend is something that many companies are willing to embrace is simple,” says Chaudhry. “Investing in mobility boosts worker productivity and, in turn, yields competitive advantage, shorter product and sales cycles, and real revenue gains.” And, the more mobile workers a company has, the more potential revenue can grow.

“What we are seeing with customers is that this consumerization of IT is now going beyond BYOD,” he says. “Not only are employees using their personal devices for business, many times they are using their personal apps (bring-your-own-apps, or BYOA) for business as well.”

Employees are also storing and syncing corporate data to consumer-based public cloud services (bring-your-own-cloud, or BYOC) so they can share them with others. “If IT doesn’t offer them a controlled way to do this, employees will continue to find insecure workarounds — not necessarily with malicious intent, but just to get their work done,” Chaudhry says. “The result is that the consumerization of IT is going beyond BYOD and now equates to BYOD+BYOA+BYOC or, simply put, bring-your-own-IT, or BYOIT.”

For enterprises attempting to capitalize on BYOD, Chaudhry says the future is in management solutions to protect the device, combined with secure collaboration solutions to protect the data. Companies are taking these steps, he says, with the overall goal of preventing data leakage and noncompliance risks that come with the free flow of corporate information to the public cloud through personal, consumer-based accounts. “Often these personal accounts remain with workers when they leave a company, causing additional data liability risks,” he says.

Controlled solutions
In fact, Chaudhry says Copius is conducting its own research, and early indications show that around 40 percent of large enterprises are planning some sort of initiative to put in place a controlled solution to let employees securely access, sync and share documents via mobile devices, he says.

Chad Udell, managing director of Float Mobile Learning, a Morton, Ill.-based consulting firm, also sees companies moving toward broad solutions. “When considering a BYOD policy, organizations are increasingly looking toward mobile device management (MDM) and mobile application management (MAM) solutions,” he says. These technologies let one use an application and device configuration profile to the user’s advantage, requiring users to log in order to unlock devices when one employs this sort of policy, he says.

“One also can enforce data encryption on the device,” Udell says. “The bottom line is, if you are going to allow users to bring in their own devices, you’ll at least need some say in how they are configured to access network resources and work data. However, the story may be somewhat different at smaller organizations. According to Vince Plaza, vice president of IT for TeamLogic IT, a national IT support company based in Mission Viejo, Calif., small and midsize businesses (SMBs) are really only starting to think about security when it comes to the BYOD phenomenon. “Some are taking the approach that these are personal devices over which they can’t enforce too much security,” he says. But others are starting to think that even though these may be personal devices, if they are used to access company information, then companies should be able to dictate security requirements, he says.

Best practices evolve
What should enterprises enlist to deal with BYOD? Plaza says the first best practice to implement is a clear and direct security policy with definitions for proper use and access to company data. “Without this, [companies] are unable to effectively deploy other security best practices,” he says. This policy must be agreed to by the employees and it must be enforced, he adds.

The bring-your-own-device trend is expanding to applications and the cloud, thus opening holes in enterprise security, reports Alan Earls.

BYOD: A legal eye
Andrew Serwin, chairman of the privacy, security & information management practice at law firm Foley & Larnder LLP, says companies are focusing on the issue of BYOD more because it is seen as a way to reduce costs and give workers some flexibility. However, he warns, it does require more consistency and coverage in IT security policies and procedures, and some flexibility with planning, particularly around data retention. Organizations “must have clear monitoring and records retention policies,” he says. “They must also make sure that there are adequate security policies and settings on the devices.”

BYOD presents challenges, too, when it comes to compliance. Serwin says many organizations are trying to be flexible in the application of records retention and monitoring, while also balancing the legal requirements under which they operate. For certain, it is a fine line to walk.
Then, interestingly enough, Plaza says the next area of focus should be much the same as with a company laptop or desktop – namely requiring a security passcode to unlock a device, security software (anti-virus/anti-malware) on the device, use of VPNs to connect to company servers if remote connections are desired, and the ability to lock and/or remote wipe a device in case it is stolen.

Depending on their position on privacy, companies could consider a number of things not usually associated with laptops – for example, the ability to track or locate a device.

A good piece to implement is an acceptable use policy when engaging company network resources for personal devices, says Float Mobile Learning’s Udell. Terms of agreement that must be signed by the users are also crucial. “Depending on where your business resides, these agreements may need verbiage in them that protects you from liability in other areas,” he says. Thus, it is best to check with a legal adviser before moving ahead, he says.

Another easy way to begin implementation is the creation or adoption of a mandatory custom application, deployed for all devices, that checks for configurations prior to allowing access to network resources or applications, says Udell.

**Not so fast**

However, Veracode’s Shields says there is no easy, one-size-fits-all approach. The recommended level of security to put in place is a measurement of risk versus perceived benefit in user efficiency and convenience. “Depending on the culture and required security of the organization, there is a differing level of need,” he says.

No one product can deliver all of those capabilities, he says. “A successful BYOD strategy generally uses some combination of MDM, enterprise application stores, mobile anti-virus and mobile application security services,” he says.

Speaking about his own experience at MasterCard, Aguilar refers to several of the specific terms and conditions each user signs off on before being allowed to participate in the BYOD program. For example, in the event a device is lost or stolen, or an employee is terminated, corporate data will be removed from the handheld. Additionally, the BYOD program is responsible for the costs and expenses related to use.

**BYOD: Before implementing**

Tyler Shields, senior security researcher at Veracode, says some of the areas that must be addressed by an organization considering the deployment of BYOD strategy are:

**Distribution**

The ability to manage and support mobile use includes securing, deploying, installing, updating, deleting and blocking mobile applications.

**Policy**

Development, control and operation of the enterprise mobile policy.

**Accounting**

Inventory, provisioning and support of device deployment.

**Security**

Enforcement of standard device security, authentication and encryption.

**Service**

Rating of effectiveness of the underlying services to the devices.

Source: Veracode

Then, in the event that the software has not been used in 90 days, corporate data will be removed from the device. Finally, in connection with their participation, users must take “reasonable steps” to protect the data on their personal device.

John Udsher, vice president of products and marketing at AppCentra, a San Francisco-based mobile applications management company, applauds the idea of having a written policy that employees acknowledge and sign. “There should be total clarity around the organization’s expectations of how a device, the apps and data should be used and protected,” he says.

But, what happens in the event that a device is lost or stolen? “This should be clear to all involved,” he says. “Focus on what’s important – the data, how it’s used, why and when it’s of value, how it might need to be protected,” he says.

McAfee’s Siems adds one more note of caution. She says protection shouldn’t focus just on managing devices should they be lost or stolen. While that’s important, she says the sudden rise over the past two quarters of malware on Android devices makes it imperative to scan for bad code and to understand what data is being exposed through apps on the device, she says.

**Turning to technology**

What types of technologies can support BYOD risk management and security planning? For device protection, enterprises can opt for a MDM solution, says Copin’s Chaudhry. However, for collaboration, he says most industry analysts recommend providing a secure, controlled, enterprise-grade to avoid the risks of data leakage, non-compliance and version conflicts.

Chaudhry says that to be productive, employees must be able to securely and natively access, sync and share their documents from any mobile device – across any platform – from laptops to SharePoint or other file servers. Likewise, mobile workers need the most up-to-date information at their fingertips across their multiple devices. “The collaboration solution also needs to be easy for them to use,” Chaudhry says. “They shouldn’t have to remember if they stored a document in an extra mobile-specific workspace.”

That’s a starting point. But Chaudhry says there are more things to consider. For example, he argues that employees should also be able to work on their documents with productivity apps with which they are familiar – the apps that are native and appropriate to the device they are using.

For example, on their tablets, they might use Quickoffice, whereas for their laptops they might prefer Microsoft Office. So, supporting those options is crucial.

Logically, they, end-to-end data governance is a must, along with robust document lifecycle policies and reporting that include a full auditing capability. “This is a must-have and will help put control back in IT’s hands and avoid liabilities,” Chaudhry says.

Further, he says IT administrators should look for a solution that allows documents to be shared by trusted applications that are authorized by an IT administrator, and avoid solutions with VPN access, which can result in too many security challenges (such as exposing corporate data to hackers, malware and more). “For enterprise-wide mobility that may span the globe, enterprises should consider solutions that can scale to tens of thousands of mobile workers, hundreds of remote sites and millions of documents,” Chaudhry says.

Fortunately, says TeamLogic IT’s Plaza, at least some of those capabilities may be available directly from the mobile carriers. For example, MDM can be a service that is added on to a device when it is purchased from the major carriers in some cases. “However, these services are not necessarily easy for the IT provider to manage across a wide range of customers,” he says.

Additionally, the software requires a password to access the data and automatically logs out after 30 minutes of non-use. “These security features minimize risk and keep corporate data secure,” he says.

Exactly what is the best combination of the numerous mobile technologies available to help in this regard will vary depending on the security posture of the organization, which industry they are in, which pertinent regulatory requirements exist, whether the firm intends to work with business partners, and so on, says AppCentral’s Dashier. The challenge of working with business partners is especially important and often overlooked, he says. “Some technologies simply won’t work for devices owned by people that don’t work for you directly,” he says. “Your business partner isn’t about to let you invade his/ her device and put MDM on it, so you need to think about how you intend to provide access, distribute, update and control the apps and data you share.”

**Who do you use for your mobile device management?**

- 8% MobileIron
- 41% Good Technology
- 50% Other

Of IT professionals polled believe mobile poses the greatest cyber threat to their organization. – Source: CDW

**Enterprise surety**

**Focus on what’s important – the data...**

— John Dashier, VP, products and marketing at AppCentral
Last of all, Udell recommends thinking about mobile device forensics—an emerging field in which security experts are tasked with cracking into devices and attempting to access what is thought to be secure information. Additionally, he says, companies significantly reduce their risk profiles by monitoring their mobile platforms’ recommended best practices policies and continuing to require that their internal developers and vendors adhere to them in their development efforts.

Address compliance requirements, Chaudhry says enterprises must continuously monitor the state of each device accessing the network, whether it is approved or not. “They are checking the network, whether it is approved or not. ‘They are checking to require that their internal developers and vendors adhere to them in their development efforts. They are checking whether devices are in compliance with corporate policies, if there are new apps, and they are refining their policies based on what they see,” he says.

Whether the concern is Sarbanes-Oxley, the Patriot Act, the EU Data Protection Directive, or industry-specific mandates, such as the Payment Card Industry (PCI) standard or the Health Insurance Portability and Accountability Act (HIPAA), Chaudhry says organizations need enterprise-grade solutions that give IT the controls to ensure compliance.

Eliminating risk
Key elements for an architecture that meets IT compliance include secure access that does not require IT to open ports in the firewall or duplicate repository data to a mobile-specific workspace in the DMZ or cloud, says Chaudhry. This framework also makes it necessary to eliminate the risk of rogue apps and backdoor infiltration or malware exposure. This architecture should also provide a secure “container” that isolates and protects company documents on the device and trusted app sharing with corporate or authorized third-party applications.

In Chaudhry’s view, robust policy management should include existing file-server-environment permissions and Active Directory policies, as well as comprehensive mobile-specific policies that provide for end-to-end governance, reporting on mobile workloads, including auditing capabilities; multi-factor authentication verifying the user and device; 256-bit encryption for data travelling over the air and at rest; and passcode protection, corporate data wipe and access-revoking for lost or stolen devices.

BYOD: Best practices
Punmesh Chaudhry, co-founder and CEO of a Marlborough, Mass.-based Coplan, a provider of mobile collaboration solutions, says there are some general best practices that need to be followed by companies and organizations embracing BYOD. He includes:

1. Provide simple workable solutions that are intuitive and easy for mobile workers of varying adeptness to use.
2. Protect sensitive and personal information. Identify personal and corporate data so that you are not infringing on privacy laws and at the same time can protect your corporate data.
3. Isolate corporate data on the device and ensure compliance with governance policies for what can be done with business documents.
4. Implement end-to-end governance of all business data to ensure you have protection and records management.
5. Continuously monitor automated actions to ensure compliance with corporate policies and regulations.
6. Ensure that you have a way to deal with departing employees and how mechanisms, such as remote wipe and passcode protection, for lost devices.

Source: Coplan

“Being able to understand what corporate data is on the personal device and what the device profile is—to allow or prevent corporate access—helps IT maintain and enforce compliance,” says McAfee’s Siems. “It also enables IT to take the appropriate next steps when a device is lost or stolen to prevent security breaches and data loss.”

Here again, though, Plaza says SMBs may be behind the curve. “This is still a learning process for the SMB since the BYOD phenomenon has grown exponentially compared to other technologies,” he says. “It has been a disruptive technology in that the IT leader/provider for the SMB has to play catch up to try and ensure that security is not compromised by the desire for ease of access.”

In the final analysis, though, BYOD may be simply too challenging for some kinds of organizations. “There are some industries that might have to say ‘no’ to BYOD,” says Dasher. For instance, defense organizations may not be able to achieve their security requirements with BYOD. Likewise, he says, finance has long relied on Blackberry and the venerable BlackBerry Enterprise Server. “The strict governance that guides the financial community may force them to only support certain platforms or devices,” he says. “It’s really case by case. The employees who work in these heavily regulated industries generally understand that there is inherently less latitude for unchecked BYOD.

But, rest assured that organizations will test the BYOD waters and figure out what works and what doesn’t. As such, industry observers are confident that BYOD is not going away. ■

This article originally ran in a Spotlight edition of SC Magazine.

“Being able to understand what corporate data is on the personal device and what the device profile is—to allow or prevent corporate access—helps IT maintain and enforce compliance,” says McAfee’s Siems. “It also enables IT to take the appropriate next steps when a device is lost or stolen to prevent security breaches and data loss.”

Here again, though, Plaza says SMBs may be behind the curve. “This is still a learning process for the SMB since the BYOD phenomenon has grown exponentially compared to other technologies,” he says. “It has been a disruptive technology in that the IT leader/provider for the SMB has to play catch up to try and ensure that security is not compromised by the desire for ease of access.”

In the final analysis, though, BYOD may be simply too challenging for some kinds of organizations. “There are some industries that might have to say ‘no’ to BYOD,” says Dasher. For instance, defense organizations may not be able to achieve their security requirements with BYOD. Likewise, he says, finance has long relied on Blackberry and the venerable BlackBerry Enterprise Server. “The strict governance that guides the financial community may force them to only support certain platforms or devices,” he says. “It’s really case by case. The employees who work in these heavily regulated industries generally understand that there is inherently less latitude for unchecked BYOD.

But, rest assured that organizations will test the BYOD waters and figure out what works and what doesn’t. As such, industry observers are confident that BYOD is not going away. ■

This article originally ran in a Spotlight edition of SC Magazine.

How 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 all basic functions to a satisfactory level. A “C” on the product’s report card.
★★ Fails to complete certain basic functions. A “D” on the product’s report card.

How we test and score the products
Our testing team includes SC Magazine Labs staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme based on a pre-determined 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 Regional and National Security at Eastern Michigan University. We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 15488) 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 of the tester and are validated by the technology editor.

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

What the recognition means
Best Buy goes to products the SC Lab ranks as outstanding. Recommended means the product has shone in a specific area.

Lab Approved is awarded to extraordinary standards that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

How 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 all basic functions to a satisfactory level. A “C” on the product’s report card.
★★ Fails to complete certain basic functions. A “D” on the product’s report card.

How we test and score the products
Our testing team includes SC Magazine Labs staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme based on a pre-determined 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 Regional and National Security at Eastern Michigan University. We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 15488) 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 of the tester and are validated by the technology editor.

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

What the recognition means
Best Buy goes to products the SC Lab ranks as outstanding. Recommended means the product has shone in a specific area.

Lab Approved is awarded to extraordinary standards that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

What the recognition means
Best Buy goes to products the SC Lab ranks as outstanding. Recommended means the product has shone in a specific area.

Lab Approved is awarded to extraordinary standards that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.
Database & application security

While we did not see a lot of encryption in this set of products, these tools can severely curtail the complexity of attacks against applications, says Peter Stephenson.

When we talk about database and application security we are faced with a major challenge: It is difficult, apparently, to define what the terms include. Also, it is important to differentiate between the two definitions. Are database and application security the same things? Are they different? How and why? A quick browse of the web will not turn up many answers. Compare scholarly papers, vendor specifications and university presentation slides and one comes away with a hodgepodge of information. We saw a bit of that vagueness as we looked at application and database security products. So, let’s begin by defining a few things. The best security when it comes to data — whether in a database or as part of an application — is encryption. Interestingly, we did not see a lot of that this month. In fact, most of the tools’ emphasis was on using application firewalls to keep the bad guys away from the data in the first place.

The notion of application firewalls is not new. The complexity of attacks against applications, however, is growing at a serious pace. Fault and vulnerability testing of applications is better than ever. However, that doesn’t help much if you don’t perform the testing during the development phase of internal products, of course. Also, there are lots of software applications that we use, but we did not develop. If those products are on our network and they have vulnerabilities, they could be a covert channel into your enterprise. So why not add encryption? That depends on to what you are adding encryption. It is practical to add encryption to a database, but to a front-end application, perhaps not so much. Even with databases there is a problem. Encryption keeps the bad guys out of the database — unless they are hijacking a session. That, naturally, is because the database is open, the user is connected and the traffic is in clear text. Now, suppose that our bad guy somehow gets the password and spoofs a legitimate user? If your only protection is encryption — no matter how strong it is — the data is exposed and, if the bad guy can gain access, you will lose it. So there is a very good rationale for using some form of application firewall to keep data thieves at bay. Having encryption is not a bad thing, though. With today’s distributed architectures and fuzzy perimeters, defense-in-depth never has been more important. The way defense-in-depth is implemented on current enterprises is very heterogeneous. It may include a network firewall, an application firewall, data leakage protection at the gateway and the endpoint, encryption and application or web firewalls. The idea is that we need to protect the data wherever it lies, as well as in transit.

We were generally quite pleased with the functionality and feature sets of these products, and our sense is that this is a good representative mix for the type. Occasionally, we saw some narrowness in the feature set, but overall that was unusual. Support, as a rule, is solid and deployment straightforward. When buying a product from this group be careful that it supports both a current and planned database deployment. Don’t forget that there are, in many organizations — as well as in applications — versions of SQL that are not made by Microsoft or Oracle.

Architecture also is important. Look at where the product fits best, per the manufacturer’s recommendation, into the architecture. Then, assess whether that is practical in the enterprise. These products should be part of an overall strategy, so if you are using a lot of software/hardware devices to protect the enterprise (IDS/IPS, firewall and more), make certain that your new application firewall is compatible.

Finally, there are application security devices, database security products and combinations of both. Check to see if you need one or both environments protected to make sure that your choice does exactly what you need. These can be tricky beasts to buy and deploy, but with just a bit of care and pre-planning you should be good to go.

Gain the security skills and IT certs the industry demands...

Online.

Become an IT security expert with a bachelor’s or master’s degree in IT security from WGU.

- **Accredited Degrees AND Certifications** — WGU offers both an accredited bachelor’s and master’s degree program in IT security, both of which incorporate recognized IT security certifications without adding classes or costs.
- **Opportunity to Advance Quickly** — A competency-based approach to education that allows you to leverage prior experience and your IT certifications to complete your degree faster.
- **Flexible Online Learning** — Log in and learn anytime, anywhere you can find the time.

Programs begin the first of every month. A smarter way to reach your future can start right now!

Learn more: Call toll-free 1-866-225-5948 or go to www.wgu.edu/scm.
Application Security DbProtect

Focusing solely on database security, DbProtect from Application Security is an affordable database security product which, given the right environment, could be very beneficial to administrators.

Product installation was reminiscent of a Snort deployment, in that a central console is first installed - which contains the management interface and the analysis engine – with sensor nodes to follow. Starting with the console, the product documentation stated that 64-bit Windows Server 2003 R2 or later with 8 GB RAM and 20 GB of disk space were required, although Application Security recommends 100GB as the analytics engine can use a great deal of space generating reports. MS SQL 2005 or later was also required, but Express editions are not supported, so non-Microsoft shops will be looking at an extra expenditure.

That said, the product relies on a number of other components. The installer scanned our fresh Windows Server 2008 system and was able to install its own required components. However, we did have to upgrade the target platform to 12 GB RAM and 75 GB of drive space before installation was successful. The host-based sensor deployment was a manual process – we had to logon to each of our database servers and install the sensor, then register that sensor to the console. We initially had trouble connecting our sensors to the console, until we determined that we needed to disable IPv6 support on the network interfaces of the involved systems. All in all, it took a couple of hours to get everything installed and communicating properly.

Supporting Microsoft SQL, Oracle, DB2 and Sybase (notably, MySQL is absent), DbProtect functions primarily as a database intrusion detection system (IDS), with a few intrusion prevention systems (IPS) features built into its Active Response system - configurable automated actions triggered by policy violations. While disabled by default, the IPS features allow for connection termination or database user account locking, as well as the triggering of user-specific events. The product uses a modular deployment methodology featuring a central console with both host- and network-based sensors available for gathering data. The host-based sensors appear to be much more mature, as the number and type of databases supported by the network-based sensors is more limited. Check the product documentation carefully, however, as some database products require one or the other; for example, MS SQL shops will need to install a host-based sensor on their database server as the network sensor is not supported, but older versions of Oracle require the use of a network sensor.

We were quite pleased with the DbProtect documentation. A number of manuals were available, including installation, administrator’s, sensor configuration and user’s guides. Each was a well-crafted PDF with numerous screen shots and plenty of bookmarks and hyperlinks, which made navigation easy.

For the package reviewed here, the retail cost is $5,100, which includes the vulnerability, rights and activity monitoring modules. Each of those is available for purchase separately – with Vulnerability Monitoring and Rights Management available at $1,500 each, and Activity Monitoring available at $2,100. Support starts at 20 percent of the license fee for standard eight-hours-a-day/ five-days-a-week assistance renewable on a yearly basis.

Barracuda Networks – Barracuda Web Application Firewall 460

Relatively inexpensive, but with a strong feature set, the Barracuda Web Application Firewall provides affordable security without skimping on features or breaking the bank. Shipped as a rack-mountable appliance, Barracuda made setup of the device extremely simple. Following the quick-start guide, it was a simple matter of setting our interface IP’s, updating the firmware and configuring a service – all completely straightforward. From unboxing to completing our first policy configuration, we were up and running in about 15 minutes.

Anyone who has used a Barracuda Networks product in the past will instantly be familiar with the user interface. A clean statistical dashboard is presented on logging in, and all device configuration categories are arranged in tabs across the top. By hovering over each tab, the relevant subcategories are displayed. Administrators can get from one configuration or report page to any other with a single click. Multiple administrator roles can be defined with granular control allowed per user over which configuration and report screens to display. The device can be deployed in the industry standard reverse proxy mode, a bridge path mode or one-armed proxy mode. Although we chose to go the reverse proxy route, we liked the flexibility the device offered.

The product supports application acceleration and content caching and offers an implementation of SSL offloading it calls InstantSSL, which functions as one would expect. Some of the solution’s default policies include parameter attack filtering against SQL injection, OS command injections, directory traversal, XSS and others, digital signing or encryption of cookies, server error suppression, file extension blocking, request sizing limits and cookie replay protection.

The product offers traffic monitoring in a passive mode, allowing administrators to observe violation reports and adjust policies if false positives are detected. An automated policy tuner integrates with the firewall logs and generates exceptions or tunes existing policies. The policy tuner also allows granular rules to be created governing specific portions of a web application, such as a web form.

We were pleased with Barracuda’s documentation. The two-page quick-start guide gave us everything we needed to have a basic configuration in minutes. The website offers more in-depth administrator’s guides, a best practices guide, and a variety of whitepapers. Everything was well organized and easy to find.

The product ships with basic support included, which gives users eight-hours-a-day/five-days-a-week phone and email support and a year’s worth of enterprise updates. For an additional yearly fee, administrators can purchase the company’s enhanced support package, which includes 24/7 phone and email support and hardware replacement within one business day.

The cost of Barracuda’s enhanced support package is $1,549 per year. We would have liked to see a 24-hour replacement option instead of just one business day. But, the price per unit is almost low enough to keep a spare on hand. At a cost of $8,898, the Barracuda Web Application Firewall is a solid value.
Bayshore Networks SingleKey

SingleKey from Bayshore Networks is a full-featured application firewall that provides solid protection from malicious attacks to enterprise applications. This product provides defense to a vast number of application types and protocols, including HTTP/HTTPS, non-web internal protocols, databases, email, lightweight directory access protocol (LDAP), user datagram protocol (UDP) and FTP, as well as quite a few SCADA protocols.

SingleKey is provided as a highly configurable hardware- or software-based appliance, which we found to be quite easy to use. The initial setup of the appliance consists of connecting it to the network and browsing to the default IP address using a web browser on a network machine. Once at the web-based management console screen, we were able to login using the default credentials for the administrative user. After logging in, we noticed that this product comes as a complete blank slate and there is a lot of configuration to be done. All configuration is done manually without the help of wizards or templates.

With that said, this solution has a lot to offer in the way of configurability. We found the management interface to be easy and intuitive to navigate and we were setting up policies for applications within minutes of turning the appliance on. On top of a solid policy engine, this tool also includes some excellent built-in heuristic capabilities. SingleKey can automatically create a baseline of behavioral patterns of an application that is being monitored. This analysis is then stored in a backend database to be used to detect behavioral anomalies in real time, which can indicate that an application is under attack. Aside from baselining heuristics, this product also features a heuristic learning mode. Using this, administrators can automatically define internal policy rules to match the characteristics of the applications being protected with specific granularity.

Documentation included setup, installation and user guides. The installation guide covers installation of the software-based appliance with clear step-by-step instructions and screen shots of the deployment steps. The user guide, on the other hand, is not as detailed. This basically provides an overview of the various screens and menus of the administration console with a few examples, but there are no configuration instructions or context to the examples provided. We would have liked to see a lot more detail on how to configure policy and manage the appliance.

Bayshore Networks offers support through annual maintenance plans. Customers can purchase standard business-hour support or gold level 24/7 support at $1,100 and $1,375, respectively. These offers include both phone- and email-based technical aid, as well as access to an online customer support portal. This offers customers access to a support wiki, as well as other helpful information.

At a price starting at around $32,000 for the hardware appliance, this tool is a pricey investment. However, we find it to be a reasonable value for the money based on its overall combination of highly configurable policy options and heuristics-based learning and baselining features. It is designed for a large environment that includes sensitive applications that need solid proactive protection from threats and malicious attacks.

F5 Networks BIG-IP Application Security Manager

Although they're primarily known for top-shelf networking products, F5 Networks' offerings in the application security space is no afterthought. Available as a standalone appliance or module for one of its network products, the BIG-IP Application Security Manager (ASM) functions as an application firewall, protecting web applications and services with a powerful policy engine.

The initial setup was reasonably straightforward. The product we received for review was bundled with the BIG-IP Local Traffic Manager, which complicated the network setup only slightly. After defining our interfaces and assigning IP address and VLANS, we were ready to define our first policy. Policy creation was deceptively simple. The ASM offers a wizard for creating policies and came packaged with a number of predefined templates for several of the more popular web application packages, including Microsoft Outlook Web Access, SAP NetWeaver, PeopleSoft and others. We needed only to specify the virtual IP of the application, enable the appropriate template and apply the policy.

The core of the ASM is the application firewall. Providing extremely granular rule options, the tool allows administrators to control HTTP responses at a parameter level – each parameter can be checked for length, attack signatures and more. It offers a good bit of data leakage protection, too, as it can scan HTTP responses for defined bits of data, blocking or masking that data as appropriate. It also provides protection against denial-of-service attacks. The ASM's Policy Builder option is a strong feature. Designed to run on live production traffic, this system listens to normal traffic and builds a custom policy around what it sees, applying the appropriate signatures automatically. Customers of WhiteHat Sentinel or Cenzic are able to take advantage of the ASM's virtual patching feature, which allows them to import their vulnerability assessment reports and have mitigation rules automatically created.

If power and flexibility are the ASM's strengths, documentation is its weakness. While we can't disparage the accuracy and volume of the documentation, our issue is with its presentation. The vast majority of the documentation is up on F5's website as HTML or PDF documents. That in and of itself is fine. However, the sheer volume can make it challenging to find the document with the information for which one is looking, especially considering how fragmented it is. It has clearly been organized with a bend toward answering specific questions instead of offering general help. This is great for existing users, but makes getting started a little more difficult than it should be. We would have preferred a solid start-to-finish blocking guide. Unfortunately, we were forced to pick our way through a number of different PDFs and HTML documents, slowly assembling our own installation manual. That being said, we couldn't come up with any question that F5 didn't have a documented answer for either in its manuals or the AskF5 knowledge base, so they are nothing if not thorough and we appreciated that.

The base cost of the ASM hardware and licensing is $14,995. Support costs start at 12 percent of the retail price of the product. All F5 solutions come with a one-year hardware warranty.
Fortinet FortiDB-400c

Given the importance of the data contained within any corporation’s databases, the task of keeping that data safe should be a top priority for any IT security team. Fortinet’s FortiDB-400c is dedicated to helping security professionals do precisely that.

For such a feature-rich device, setup was easy. After setting up the interface IPs and updating the firmware, we were ready to begin monitoring our first database. Database servers were referred to as targets during setup, and we defined these by selecting the database server type (in our case, Microsoft SQL), the server IP and the username and password of an account on that server. We were given the option to connect at a server or database level. We chose to connect at a server level, although we appreciated the granularity offered. By making use of the product’s autodiscovery feature, we only had to specify an IP range, database type and a port range and the device scanned our network and automatically found and added our SQL server to the list of monitored targets.

Focusing solely on database protection, the FortiDB-400c has a wide array of features allowing administrators to control precisely when and what database services are being accessed and who is accessing those services. The device offers easy black- or whitelisting based on user, application or IP address. It monitors all database activities, including data manipulation queries, such as select, insert and update; data definition language queries, such as create, alter and drop; and data control language queries, such as grant and revoke. Based on the policies that administrators define governing those queries, the device can issue transmission control protocol (TCP) reset packets in the event of policy violations via its database firewall feature. It offers built-in vulnerability assessment tools, which can be scheduled to run at any interval, and automatically generate reports, which can be sent to database administrators or anyone responsible for database security. Report and monitoring data can be archived off the device via its archive scheduler. However, there does not appear to be a way to archive the device configuration itself without using the command line interface and an FTP server. It’s a small nitpick, but we would have liked to be able to perform all device maintenance via the GUI. The device comes preconfigured with a number of auditing and compliance reports, and custom reports are easy to create. The tool supports multiple administrator profiles with roles defined for reporting, security and database target and policy management.

Fortinet offers eight-hours-a-day/five-days-a-week or 24/7 support options, which it supplies via phone or web chat. Administrators who subscribe to the Advance Support program are assigned a technical account manager, making it even easier to get the help needed. Fortinet also demonstrates a high level of confidence in its product, offering free basic-level support for proof-of-concept deployments. Adding to that, it maintains a sizeable knowledge base and user support forums on its website.

Base price for the FortiDB-400c is $14,995, plus $2,249 per year for upgrades and eight-hours-a-day/five-days-a-week support, or $3,749 per year for upgrades with 24/7 support.

Imperva SecureSphere Business Security Suite

With large enterprise networks under constant attack from malicious entities, administrators need powerful defenses. With what may just be the Cadillac of application and database security products, Imperva makes its appearance to help hold attackers at bay. Just prepare your checkbook, this Caddy doesn’t come cheap.

While Imperva supports running the SecureSphere software in a multitude of configurations, both virtual and physical, the product was delivered to us as a pair of appliances – a dedicated management server and a gateway device. The setup process was not insurmountably complex. However, we did need to contact support in order to acquire the administrator’s guide before we could make much progress. The appliances used a 38400 baud rate on its serial ports as opposed to the somewhat-standard 9600 baud rate we find on most networking gear, so we had to check the admin guide for those settings. The product’s configuration was split between the command line interface (CLI) and the web interface on the management device, with all networking configuration being done via the CLI, as well as linking the gateway to the management device. There was a decent menu-driven system, so we didn’t find ourselves typing out long commands. All other functionality was set up via the management server’s web interface, so after the initial setup we didn’t need to go back to the CLI again.

SecureSphere has far more functionality than we could possibly cover here in the space allotted. Functioning primarily as an application and database firewall with IDS/IPS features, the solution is deployable in a number of different configurations, with support for deployment as an inline gateway, as a reverse proxy or as a network sniffer. The offering supports SSL offloading and decryption of SSL traffic, input validation, application user tracking, session/cookie protection and more. Attack signatures are automatically updated from the Imperva website, and the product supports user-created signatures as well, using a proprietary language resembling that used by Snort. In addition to the standard attack signature detection methodology, subscribers to Imperva’s ThreatRadar service get the added benefit of reputation-based IP blocking. On the database side, the product supports activity auditing, continuously monitoring target databases and maintaining an audit trail. It also can alert on and/or block unauthorized access attempts and perform user rights analysis.

The documentation is stellar. The administrator’s guide covers everything from deployment planning to product configuration, with network diagrams and screen shots where appropriate. The user’s guide covers day-to-day tasks, including reporting, detection signature writing, user tracking and more. Both manuals come as well-formatted PDF files.

Imperva offers three tiers of support. Standard includes help from 8 a.m. to 6 p.m., Monday through Friday, while the enhanced tier extends those hours to 24/7. The premium support package includes advanced hardware replacement. At a base price of $51,000, buying into the SecureSphere platform isn’t cheap. Support costs start at $7,650 for the standard support package.

Fortinet FortiDB-400c

Strengths
Comprehensive feature set
Solid platform
Excellent value for money

Weaknesses
Some functions require the command-line interface, but that’s a nitpick.

Documentation
Support
Ease of use
Performance

Value for money

OVERALL RATING ★★★★★

Imperva SecureSphere Business Security Suite

Strengths
Enormous feature set
Flexible deployment options.

Weaknesses
High cost and slightly more complex setup.

Ease of use
Performance
Documentation
Support

Value for money

OVERALL RATING ★★★★★
McAfee Database Activity Monitoring

Database Activity Monitoring from McAfee provides both threat protection as well as database auditing for compliance needs. Right out of the box this product can scan the environment and find databases automatically and protect them with an array of preconfigured security policies. Furthermore, this tool also features the ability to help administrators design and build a customized policy that provides the correct protection for the needs of the environment.

We found this solution to be simple to deploy and configure. The initial installation was done by running the server installation executable. Once the installer was launched, we were taken through a brief setup wizard, which helped us configure the ports necessary for installation, as well as a few other settings. After the install was complete, we were able to access the web-based management console. After we logged into the management console for the first time, we were taken to a menu in which we could scan the network for databases or add them manually. This was pretty much the end of the initial configuration and we were then able to start creating policy and managing security options. We found the management console to be well-organized and intuitive to navigate. However, it does include a lot of functionality, so there are several menus and screens through which to navigate.

Highly configurable security policies drive this product. The Database Activity Monitoring server can monitor activity locally on each protected database and alert or terminate suspected malicious activity in real time, along with blocking possible attacks against unpatched databases. This product also provides a full audit trail of possible malicious activity – even by privileged users. Along with being highly configurable, this offering also provides support for a wide array of databases, including Oracle, Microsoft SQL Server, Teradata, MySQL, IBM DB2 LUW and Sybase ASE. All these can be monitored, protected and audited by the Database Activity Monitor.

Documentation included installation and administrator’s guides. The installation guide provided an excellent amount of detail on how to install the product, along with initial configuration instructions. The full administrator’s guide offered configuration and management instructions and clear step-by-step configuration procedures. However, both guides lacked screen shots and visuals, which we find make configuring and managing products easier and more intuitive.

McAfee includes the first year of support in the initial purchase price. After the first year, customers can purchase additional assistance as part of an annual agreement at a cost of 20 percent of the purchase price. Support offers includes 24/7 phone- and email-based technical support, as well as access to a large online support area.

At a price starting at around $5,000 with the first year of support included, we find this solution to be an excellent value for the money. McAfee Database Activity Monitoring provides a solid set of features for monitoring, protecting and auditing databases across the enterprise while being easy to use and manage.

Classy classification

Every now and then, we get a chance to make lemonade out of a lemon. Usually, the lemon is of our own making. It doesn’t happen often. In fact, as long as I’ve been writing for this magazine, I’ve only seen it once before. So mark it down: this is our lemonade for this decade. The best lemonade, of course, is not just tangy... it has a pleasant sweetness to it. And so it is with this month’s First Look.

In our email security Group Test in September, we inadvertently included TITUS Message Classification – TMC – in a group with which it was more than a bit out of place. The results, as you might expect, were less than spectacular. TMC was a square peg in a very round hole, and what emerged in the review was what one might, under the circumstances, predict. I personally took a look at the product and it didn’t take me long to realize what had happened. Too late, though. The issue had been put to bed and there was no going back. With that as background, get your glass and some ice. I’m pouring.

TMC is a deceptive product at first glance. It looks like a gizmo that sticks a classification message on an email and that’s the end of it. But, that classification label is only the first of many important steps. What is most interesting to us is what happens next. TMC enforces the classification and does all of those things that are anticipated by appropriate regulatory requirements. It also integrates cleanly with third-party products and that, perhaps, is its greatest strength.

We tested TMC using Microsoft Outlook and Exchange Server. However, there are also versions for Outlook Web Access and Lotus Notes. Installation was straightforward and the policy engine was clean to configure. The product worked correctly the first time. We used a simple test bed consisting of two Exchange servers, each in its own domain and each with a single client.

TMC has a clean user interface and the manual is first rate. It’s a good thing that the manual is delivered as a PDF. If it was paper, you would need a fork lift to deliver it. We found everything we needed, but there also is a strong quick-start guide that cuts straight to the chase for those disinclined to wade through the 324 page administrator’s guide. Don’t blow the manual off completely, though. It is full of procedures and screen shots that answer just about any question you might have related to deployment.

A key difference from similar products is that the classification is carried with the message as persistent metadata, so no matter where the message ends up it carries its classification with it. Also, TMC links tightly with third-party products so that, although it does not encrypt email itself, it can invoke encryption by a third-party encryption product based on rules that users set up in TMC’s policy.

If one is doing or getting ready to do data classification, check this one out. TMC is highly configurable, easy to use and at all levels and solid integration with third-party products that enforce the classification rules. – Peter Stephenson, technology editor

**CLASSY CLASSIFICATION**

**SC BEST BUY**

**Company:** TITUS

**Website:** www.titus.com

**Price:** $26.95 per user; based on 5,000+ users, plus $6.74 per seat for annual maintenance.

**What it does:** Message classification.

**What we liked:** Creative approach to message classification and enforcement – allows the user to control message classification which, in turn, is enforced by TMC.

**What we didn’t like:** This can get a bit pricey, but for what it does that may not be a serious concern in your environment.
At SC Congress New York last month, security experts from government and the private sector discussed their strategies in defending networks, while 40 vendors showcased their latest security solutions.

At SC Congress New York last month, security professionals gathered on Oct. 11 for the fifth annual SC Congress Chicago.

S pirited discussions on everything from DDoS attacks affecting dozens of banks to the latest protection measures used in this new era of BYOD to developments in cloud security to the Department of Energy’s strategies for ensuring national networks are defended... took center stage at SC Congress New York last month.

Keynotes and panel discussions offered tips and strategies from government and private sector leaders. Forty companies were represented on the expo floor, touting the latest and greatest tools and services. And there was plenty of time for networking and socializing for the 400 attendees.

If you missed our gathering in New York, don’t despair. We are launching the inaugural SC Congress Chicago on Nov. 8. For more information, visit http://congress.scmagazine.com/chicago.

The FuTure iS now

SC Congress New York.

NOVEMBER

» Gartner Symposium/ITxpo Nov. 5-8 Disruptive technologies like cloud, social and mobile are revolutionizing business. The most successful CIOs and senior IT leaders will embrace the future by turning their attention to growth, cost reduction and competitive differentiation.

Venue: Barcelona, Spain
Contact: gartner.com

» Cloud Security Alliance Congress 2012 Nov. 6-9 This third-annual gathering is aimed at IT security professionals and executives who must further educate themselves on cloud security. In addition to offering best practices and practical solutions for ensuring secure in the cloud, this year’s conference will focus on emerging areas of growth and concern in cloud security.

Venue: Orlando, Fla.
Contact: msti.com

» SC Congress Chicago Nov. 8 SC Magazine brings its popular conference and expo event to the Windy City for the first time. As proven in New York and Toronto, SC Congress gatherings offer private and public sector information security professionals practical solutions, expert guidance and timely information to help effectively combat today’s cyber criminals. Given the huge jumps in the number and sophistication of cyber attacks, such assistance should go a long way in helping you strengthen your organization’s risk management position and tighten up needed security controls.

Venue: Chicago
Contact: scongress.com

» Gartner Symposium/ITxpo 2012 Nov. 12-15 Now more than ever, CIOs and senior IT executives must embrace new concepts, pursue new strategies and acquire new leadership skills. Gartner’s agenda for this show covers every aspect of what matters most in IT, in an array of session formats from workshops, end-user case studies, analyst-user roundtables, short-form sessions, clinics and much more.

Venue: Gold Coast, Australia
Contact: gartner.com

» Compliance Week West Nov. 15-16 This annual gathering features keynotes and panel sessions to help compliance, risk and audit executives understand not just what the issues are that fum- max their operations, but how to implement management and information systems to address those threats.

Venue: Palo Alto, Calif.
Contact: complianceweek.com

» SANS London 2012 Nov. 26-Dec. 3 SANS brings 18 courses in four disciplines to Central London. SANS training is well-known for being relevant and pragmatic. All SANS instructors are industry leaders and experts who understand the challenges you face on a daily basis.

Venue: London
Contact: www.sans.org/info/107474

2013

JANUARY

» MacWorld 2013 Jan. 31-Feb. 2 Macworld/iWorld is a popular event focused solely on the Apple products platform. Mac users and buyers, top media outlets and industry experts come to the event each year for face-to-face meetings, to witness new products, and participate in technical training and educational programs, as well as social opportunities that set the agenda for Apple.

Venue: San Francisco
Contact: digworldexpo.com

FEBRUARY

» ShmooCon 2013 Feb. 15-17 This annual East Coast hacker convention offers three days of technology demonstrations and exploitation; inventive software and hardware solutions; and open discussions of critical information security issues. The first day, called “One Track Mind,” consists of speed talks. The next two days bring three tracks: “Build It,” “Break It” and “Bring It On.”

Venue: Washington, D.C.
Contact: shmoocon.org

MAY

» ICSE 2013 May 18-26 The 35th International Conference on Software Engineering, ICSE, provides programs where researchers, practitioners and educators present, discuss and debate the most recent innovations, trends, experiences and challenges in the field of software engineering. ICSE 2013 encourages contributors from academia, industry and government to share leading-edge software engineering ideas with leaders in the field.

Venue: San Francisco
Contact: icse-conferences.org

ADVERTISER INDEX

Company

Page

URL

Axway 37 www.axwaysecurity.com

EA ST 5 www.easst.com

IBM 7 www.ibm.com

MarketScope.com 7 www.scmagazine.com

SANS Online Training 7 www.sans.org

SC Awards 2013 7 www.scmagazine.com

SANS 19 www.sans.org

Western Governors University 39 www.wgu.edu

www.scmagazine.com • November 2012 • SC 49
As more and more organizations find themselves facing advanced cyber threats, information sharing becomes more critical, yet it is still not widely practiced. The sophisticated threats facing many organizations today tend to be orchestrated by skilled and motivated threat actors. They use tools and techniques specifically designed to defeat traditional security controls, like firewalls, intrusion prevention systems and anti-virus. These actors are also very dynamic in that they generally do not use the same IP addresses, domains or malware over and over. This creates a significant challenge for the security vendors. By the time malware, malicious domain names or IP addresses are added to their security products, the threat actor has already abandoned those in favor of new ones.

This information or intelligence is commonly referred to as an indicator of compromise (IoC). In addition to those examples, an IoC could be the hash of an executable, a unique HTTP user agent string or a specific email subject line. Almost anything that could be used to identify a compromised system and searched for could be considered an IoC. There are several electronic formats that can be used to store and share IoCs. However, none of these formats is a standard.

Though standards lack, sharing threat data is vital, says EMC’s Christopher Harrington.

Today, there are pockets of sharing cyber intelligence and IoCs. Most of these are industry specific in nature. The U.S. Department of Defense (along with military contractors) has the Defense Industrial Base (DIB), the Defense Industrial Base Collaborative Information Sharing Environment (DICESE), and the Defense Security Information Exchange (DSIE). Industry verticals, like finance, have Information Sharing and Analysis Centers (ISACs). There are commercial providers of this information as well. These are not generally vertical specific, but can be expensive depending on the specific need.

There are several challenges with sharing intelligence and IoCs though. Many organizations do not want to let anyone know that they have had a cyber incident, no matter how small. It is still regarded as a mark of shame to many if one admits a breach or attack.

Traditional security technologies... do not provide the level of security needed...

While there are several electronic formats that can be used to share IoCs, there are none that could be considered a standard. Common formats, like OpenIOC, CybOX and IODEF, can be used to describe IoCs. Each one has a slightly different purpose, and they all have very different origins. Which one is best will be determined by how the IoCs are to be shared and, sometimes, with whom they are shared. Sharing of IoCs and cyber intelligence is still in its infancy. While there are services that sell this information, there are very few products that can process it. Without products to process this data, it falls on the shoulder of the security analyst. This can be a daunting task depending on the volume of IoCs that are involved.

But, we have an opportunity to turn a negative into a positive. With each cyber intrusion or email phishing campaign comes the possibility to share what you have learned with others. Traditional security technologies – while still a valuable part of the equation – do not provide the level of protection needed to counter this threat. By sharing indicators of compromise in a timely fashion with the rest of our community, we make the threat actor’s job that much harder. By making them adjust their tools and techniques more frequently, we create a larger window for us to detect and respond.

Christopher Harrington is consulting security engineer at EMC.

Visit awards.scmagazine.com to view the finalists and to reserve your tickets today.

EARLY BIRD SPECIAL! Book your table by Dec. 14 and SAVE more than $800.
YOUR ENDPOINT SECURITY SOLUTION

Buy 2 years, get the 3rd for FREE*

Purchase a new, two-year, twenty-five seats or more license of ESET Endpoint Antivirus or ESET Endpoint Security, and receive a third year for FREE!

Valid from 10/01/2012 through 01/31/2013.
*Terms and conditions apply. Please visit www.eset.com/us/q4promo for details.

ESET antivirus protection trusted by IT pros

"Over the years and throughout different tests, we’ve seen that ESET develops high-performing security solutions that have a small impact on system performance."

— Andreas Clementi, AV-Comparatives founder and chairman

Visit www.eset.com/us/business to request your FREE business trial today.