FEATURES:

OFFENSIVE LINE

Organizations are taking more of a proactive stance, says Joel Yonts, CISO at a Fortune 500 automotive supply company  P18

Watching the watchers
The intelligence community in Canada is diverse and widespread...and lacks oversight.  PC1

On fertile ground
Criminals are finding that social networking sites like Facebook are rich in data  P22
Because ‘Insider Threat’ Isn’t Stamped Across Their Foreheads:
Monitor Every Computer Activity with SPECTOR 360!

**REGULARS**

4 Editorial  Mobility breeds concern
8 Threat report  Pakistan was the top producer of zombie IP addresses last month
10 Threat stats  The records of 780,000 Utah Medicaid clients were exposed by the hack of an improperly protected server
12 Update  Ontario received a record number of privacy complaints last year, according to the province’s privacy commissioner
13 Debate  Sharing security data is the sanest way to raise the cost of entry and lower ROI for criminals and spies
14 Two minutes on…  The promise of Windows 8
15 Skills in demand  Professionals with specific infrastructure experience are needed
16 From the CISO’s desk  Let’s educate our lawmakers, by Eugene Fredriksen, CISO, Tyco International
18 Offensive line  Most security practitioners, such as Joel Yonts, CISO at a Fortune 500 automotive supply company, agree that traditional, perimeter-based security is not going to cut it anymore – at least as the primary means of preventing cyber attacks.
19 Watching the watchers  The intelligence community in Canada is diverse and widespread… and lacks oversight.
20 On fertile ground  Criminals are finding that social networking sites like Facebook are rich in data.
22 Product section  Risk management and quantification in a dynamically changing environment require tools that can take inputs from sensors around the enterprise, measure threats, balance those metrics against devices and security domains on the network, and keep track of the results.
25 Group Test: Risk and policy management  When one combines risk and policy management into a single tool, the best of both worlds is available.

**PRODUCT REVIEWS**

24 Product section  Risk measurement and quantification in a dynamically changing environment require tools that can take inputs from sensors around the enterprise, measure threats, balance those metrics against devices and security domains on the network, and keep track of the results.
25 Group Test: Risk and policy management  When one combines risk and policy management into a single tool, the best of both worlds is available.

**FEATURES**

18 Offensive line  Most security practitioners, such as Joel Yonts, CISO at a Fortune 500 automotive supply company, agree that traditional, perimeter-based security is not going to cut it anymore – at least as the primary means of preventing cyber attacks.
19 Watching the watchers  The intelligence community in Canada is diverse and widespread… and lacks oversight.
20 On fertile ground  Criminals are finding that social networking sites like Facebook are rich in data.

**SPECTOR 360**

Catch Them Red-Handed With SPECTOR 360 User Activity Monitoring

SPECTOR 360 captures every activity, including snapshot videos of the screen, at the source: the user’s PC, Mac, or laptop… automatically storing the activity data centrally for further auditing. Monitoring the endpoint addresses human behavior, arguably the riskiest aspect of any business organization.

Consider:
- The FBI calls employee theft “the fastest-growing crime in America.”
- The average data thief is a current employee.
- Industrial espionage costs U.S. businesses more than $250 billion each year.
- 43 percent of companies surveyed experienced an ‘Insider Incident.’

Guard against Insider Threat with SPECTOR 360.

Learn more today. Go to www.360RevealsAll.com to register for a FREE Evaluation.

Because you can’t address what you can’t see... and ‘Insider Threat’ isn’t stamped on their foreheads!
Editorial

Mobility breeds concern

Worries plaguing U.S.-based CSOs are pretty universal. That is, in Canada, mobile security, more advanced cyber attack methods, compliance, C-level buy-in for security, and more all are proving to be sources of stress for IT security executives there, too.

Among these, we learned at SC Congress Canada held in Toronto last month that the BYOD phenomena is still a challenging conundrum for many organizations. A Ponemon Institute study sponsored by Websense that was released earlier this year and discussed more in depth among a panel of experts during a mobile security threats session at the Toronto event seems to bear this out. Among the 4,640 IT and IT security practitioners queried for the “Global Study on Mobility Risks Survey of IT & IT Security Practitioners,” 77 percent said the use of mobile devices by employees is critical to achieving business objectives. Yet, 76 percent said these technologies put their organizations at risk.

Still, said panelist Faiza Kacem, manager for IT security and disaster recovery at the National Bank of Canada, mobile devices don’t necessarily bring new threats. Really, it’s just that the attack surface has grown because of BYOD and the use of even corporate-owned mobile devices, she explained. To deal with this properly, she suggested understanding fully all of your organization’s exposures to risks, understanding very clearly where your critical data and systems are and who/has access to them, and deploying proven security and other protective mechanisms that help to stop data leakage. Some final and important steps, she and other panelists pointed out, include staff education and the establishment and, more importantly, the enforcement of policies and procedures.

Besides these steps, Michelle Warren, founder and president of MW Research & Consulting, added that executives shouldn’t be afraid to say, “No.” After all, that’s an option if the IT security and corporate leaders feel the threats to data are just too high to risk a “yes.”

No doubt, this panel provided some strong advice and insight. Still, mobile security problems continue to vex many an IT security officer here and there.

So, now available at www.scmagazine.com, you can find our SC Spotlight on Mobile. Take a look and let us know your thoughts.

Illena Armstrong is VP, editorial director of SC Magazine.
Each month we host an event focused on protecting the crown jewels of every company – its data – enterprise defenses must be resilient. We learn from experts just what such planning entails.

ON DEMAND
Privacy and security
Most companies issue privacy and security notices assuring customers that all efforts are being made to protect their personal information and financial transactions. Yet, breaches continue to happen, wherein data is stolen and the enterprise is left to issue apologies, suffer damage to the brand, and be another more quickly and conveniently, it also introduces new vectors of attack. We offer tactics and tools to safeguard cloud implementations.

WHO’S WHO AT SC MAGAZINE

EDITORIAL
VP, EDITORIAL DIRECTOR Ilana Armstrong ilana.armstrong@haymarketmedia.com EXECUTIVE EDITOR Dan Kaplan dan.kaplan@haymarketmedia.com MANAGING EDITOR Greg Masters greg.masters@haymarketmedia.com DIGITAL CONTENT COORDINATOR Marcus Colón marcus.colon@haymarketmedia.com TECHNOLOGY EDITOR Peter Stephanoff peter.stephanoff@haymarketmedia.com SC LAB MANAGER Mike Stephanoff mike.stephanoff@haymarketmedia.com DIRECTOR OF SC LAB OPERATIONS John Alehan john.alehan@haymarketmedia.com SC LAB EDITORIAL ASSISTANT Judy Trabu Judy.trabu@haymarketmedia.com PROGRAM DIRECTOR, SC CONGRESS Eric Green eric.green@haymarketmedia.com CONTRIBUTORS
Stephen Lawton, Deb Radcliff, Jim Romeo DESIGN AND PRODUCTION ART DIRECTOR Brian Jackson brian.jackson@haymarketmedia.com VP OF PRODUCTION & MANUFACTURING John Creave john.creave@haymarketmedia.com PRODUCTION MANAGER Krissi Varbitou krissi.varbitou@haymarketmedia.com SC EVENTS EVENTS DIRECTOR Natasha Multi natasha.multi@haymarketmedia.com SENIOR EVENTS COORDINATOR Anthony Curry anthony.curry@haymarketmedia.com EVENTS COORDINATOR Maggie Keller maggie.keller@haymarketmedia.com

U.S. SALES
VP, SALES DIRECTOR David Stidman (646) 638-6008 david.stidman@haymarketmedia.com EASTERN REGION SALES MANAGER Mike Alesie (646) 638-6062 mike.alesie@haymarketmedia.com WEST COAST BUSINESS MANAGER Matthew Albertson (415) 346-6460 matthew.albertson@haymarketmedia.com NATIONAL ACCOUNT MANAGER - EVENT SALES Mike Alesie (646) 638-6062 mike.alesie@haymarketmedia.com ACCOUNT EXECUTIVE Dennis Koster (646) 638-6062 dennis.koster@haymarketmedia.com SALES CAMPAIGN MANAGER Samantha Amoroso samantha.amoroso@haymarketmedia.com SALES/EDITORIAL ASSISTANT Coco Horner coco.horner@haymarketmedia.com LICENCE & REPRINTS ACCOUNT EXECUTIVE Malika Toure (646) 638-6019 malika.toure@haymarketmedia.com EMAIL LIST RENTALS EMAIL, SENIOR ACCOUNT MANAGER Frank Cipolla, Edith Roman Associates (646) 701-3832 frank.cipolla@papertargetdirect.com CIRCULATION AUDIENCE DEVELOPMENT DIRECTOR Sherry Oommen (646) 638-6003 sherry.ommen@haymarketmedia.com CUSTOMER DATA MANAGER Joshua Blair (646) 638-6048 joshua.blair@haymarketmedia.com SUBSCRIPTION INQUIRIES CUSTOMER SERVICE: (800) 558-1703 EMAIL: info@haymarketmedia.com WEB: www.scmagazine.com/subscriptions MANAGEMENT CEO OF HAYMARKET MEDIA Lee Mancalco EXECUTIVE VICE PRESIDENT Tony Keefe

SC MAGAZINE EDITORIAL ADVISORY BOARD 2012

Rich Baich, principal, security & privacy, Dehlite and Touche
Greg Bull, global information protection and security lead partner, KPMG
Christopher Burgess, chief security officer and president, public sector, Algeus
Jaime Chanaga, managing director, CSO Board Consulting
Rufus Connell, research director, information technology, Frost & Sullivan
Dave Cullumine, chief information security officer, eBay
Mary Ann Davidson, chief security officer, Oracle
Dennis Devin, assistant vice president of information security and compliance services, George Washington University
Gerhard Eschelbeck, chief technology officer and senior vice president, Sophos
Gene Fredriksen, senior director, corporate information security officer, Tyco
International
Maurice Hampton, technical account manager, Qualys
Paul Kurtz, partner and chief operating officer, Good Harbor Consulting
Kris Lovejoy, vice president of IT risk, office of the CIO, IBM
Tim Mathias, director, information protection, KPMG
Stephen Northcutt, president, SANS Technologies Institute
Randy Sanovic, former general director, information security, General Motors
Howard Schmidt, cybersecurity coordinator, White House; former president and chief executive officer, Information Security Forum
Ariel Silverstone, former chief information security officer, Expedia
Justin Somained, chief information security officer, Yahoo
Craig Spiezio, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft
W. Hord Tipton, executive director, (ISC)²; former CIO, U.S. Department of the Interior
Amit Yoran, chief executive officer, NeStHill; former director, U.S. Department of Homeland Security’s National Cyber Security Division

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

This industry leading conference and expo addresses the most pressing issues with its one-day agenda, featuring sought-after industry experts sharing their experience and knowledge on everything from mobile security and cloud migration to hacktivism, APTs and the latest vectors of attack. We hope to see you there! For more information, click on our website: www.scmagazine.com.

For more information, please contact Natasha Mull at natasha.mulla@haymarketmedia.com. Or visit www.scmagazine.com/scwc247.

For sponsorship opportunities, contact Mike Alesie at mike.alesie@haymarketmedia.com or visit www.scmagazine.com.

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
SC WORLD CONGRESS 24/7
July 24 eSymposium: Securing the cloud
Apple and Google are ramping up their server farms to prepare for massive increases in the use of cloud platforms. While this burgeoning technology enables the quick sharing of information with one another more quickly and conveniently, it also introduces new vectors of attack. We offer tactics and tools to safeguard cloud implementations.

Who’s Who at SC Magazine
Pakistan top producer of zombie IP addresses
During the past month, the EMEA region (Europe, Middle East, Africa) was the leading source of all zombie IP addresses. Of the countries making up the EMEA, Pakistan was the top producing country. For the other regions the top producers were Brazil in South America, United States in North America and India in the Asia-Pacific region. Source: Symantec

MONTREAL – The Royal Canadian Mounted Police broke up a $200 million credit card fraud racket with the issuance of 61 arrest warrants. Authorities said the suspects stole card data from retail stores by unplugging POS systems and connecting their own devices. They retrieved the systems the following day, replaced the old ones, downloaded the stolen data and created cloned cards.

NEW YORK – An accused member of the Anonymous collective, charged recently with helping to compromise global affairs firm Stratfor, has been hit with additional charges in a new indictment unsealed here. Jeremy Hammond, 27 of Chicago, and four other defendants are charged with being part of a wider conspiracy to infiltrate corporations and government agencies worldwide.

U.K. – The organizers of the London Marathon accidentally posted on their website the personal information of the 38,000 runners in the annual race. The details exposed included email and home addresses, and involved some high-profile participants, including celebrities. The organizers corrected and apologized for the mistake, but the information commissioner is planning an investigation.

IRAN – A man who worked for payment service provider Eniak divulged the bank account details of three million residents after executives refused to heed his warning of a security vulnerability that placed customers’ data at risk. The suspect fled Iran after posting the information on his blog. He is being sought by police, and the Central Bank of Iran advised users to change their account PINs.

BERKELEY, CALIF. – Fifty students face punishment for their alleged involvement in a scam to hack the city’s high school attendance system to change grades. Four of the pupils are believed to have orchestrated the attack, and then sold access to the system so other students could expunge their absences.

PHOENIX – Phoenix Cardiac Surgery was fined $100,000 under HIPAA for failing to protect patient data when the records of more than 1,000 people accidentally were posted on the web. The five-doctor center joins an increasing number of health organizations being fined for HIPAA security and privacy violations, including BlueCross BlueShield of Tennessee, which recently was slapped with a $1.5 million penalty.

WASHINGTON, D.C. – The District’s government website – dc.gov – was briefly inaccessible after attackers launched a distributed denial-of-service attack. According to The Washington Post, someone using the alias “Cosmosis Jones” claimed responsibility and told the paper that similar attacks would continue against government sites out of support for Occupy Wall Street.

RUSSIA – Local Anonymous members temporarily drowned access to the websites of the Kremlin and President Vladimir Putin. The attackers allied with tens of thousands of protesters who took to the streets to decry the inauguration of Putin for a third, six-year term as president. The conservative Putin was president from 2000 to 2008, but became prime minister to avoid term limits.

AUSTRIA – Authorities charged a teenager with defacing and hacking 259 websites over a three-month period, ZDNet reported. The boy, 15, may have been inspired by hacktivist group Anonymous. Law enforcement officials said the suspect used widely available tools to scan sites for vulnerabilities and then exploited them. Police eventually caught up to him when his IP address briefly became visible.

IRAN – A man who worked for payment service provider Eniak divulged the bank account details of three million residents after executives refused to heed his warning of a security vulnerability that placed customers’ data at risk. The suspect fled Iran after posting the information on his blog. He is being sought by police, and the Central Bank of Iran advised users to change their account PINs.

BERKELEY, CALIF. – Fifty students face punishment for their alleged involvement in a scam to hack the city’s high school attendance system to change grades. Four of the pupils are believed to have orchestrated the attack, and then sold access to the system so other students could expunge their absences.

PHOENIX – Phoenix Cardiac Surgery was fined $100,000 under HIPAA for failing to protect patient data when the records of more than 1,000 people accidentally were posted on the web. The five-doctor center joins an increasing number of health organizations being fined for HIPAA security and privacy violations, including BlueCross BlueShield of Tennessee, which recently was slapped with a $1.5 million penalty.

WASHINGTON, D.C. – The District’s government website – dc.gov – was briefly inaccessible after attackers launched a distributed denial-of-service attack. According to The Washington Post, someone using the alias “Cosmosis Jones” claimed responsibility and told the paper that similar attacks would continue against government sites out of support for Occupy Wall Street.

U.K. – The organizers of the London Marathon accidentally posted on their website the personal information of the 38,000 runners in the annual race. The details exposed included email and home addresses, and involved some high-profile participants, including celebrities. The organizers corrected and apologized for the mistake, but the information commissioner is planning an investigation.

IRAN – A man who worked for payment service provider Eniak divulged the bank account details of three million residents after executives refused to heed his warning of a security vulnerability that placed customers’ data at risk. The suspect fled Iran after posting the information on his blog. He is being sought by police, and the Central Bank of Iran advised users to change their account PINs.
The information of 780k Medicaid clients of the Utah Department of Health was exposed

BYOD Mobile devices in the enterprise

<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>hostnoc.net</td>
<td>78</td>
</tr>
<tr>
<td>2</td>
<td>chinanet-cn</td>
<td>64</td>
</tr>
<tr>
<td>3</td>
<td>chinanet-hj</td>
<td>52</td>
</tr>
<tr>
<td>4</td>
<td>telefónica.com.ar</td>
<td>52</td>
</tr>
<tr>
<td>5</td>
<td>dacom.co.kr</td>
<td>51</td>
</tr>
<tr>
<td>6</td>
<td>uol.com.br</td>
<td>49</td>
</tr>
<tr>
<td>7</td>
<td>gxt.net.br</td>
<td>49</td>
</tr>
<tr>
<td>8</td>
<td>hitnet.net</td>
<td>49</td>
</tr>
<tr>
<td>9</td>
<td>unicom-cn</td>
<td>48</td>
</tr>
<tr>
<td>10</td>
<td>chinanet-gd</td>
<td>47</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

Spam rate compared to global email

Top attacks used by U.S. hackers
1. Chinese Infostealer trojan
2. Butterfly bot
3. Downloader trojan
4. Sinowal trojan
5. Waledac trojan

Top attacks used by foreign hackers
1. TDSS Downloader trojan
2. ZeroAccess trojan
3. Sinowal trojan
4. Alureon trojan
5. Waledac trojan

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

Top breaches of the month

Data loss

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utah Dept. of Health</td>
<td>Utah Medicaid clients had their information exposed to ransomware</td>
<td></td>
</tr>
<tr>
<td>(Salt Lake City)</td>
<td>by a hack of an improperly protected state Department of Health computer server.</td>
<td></td>
</tr>
<tr>
<td>Emory University</td>
<td>Ten backup discs that contain patient information went missing from a storage location at Emory University Hospital.</td>
<td></td>
</tr>
<tr>
<td>Hospital (Atlanta, Ga.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>South Carolina Health and Human Services</td>
<td>An employee was fired and arrested after he sent the names, addresses, phone numbers and dates of birth of Medicaid patients to his private email.</td>
<td></td>
</tr>
</tbody>
</table>

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

560,872,869 (as of May 16)

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

Internet dangers Top 10 threats

1. Silly.AT
2. VBLInject.genIF
3. Webusus.EL
4. Xtrat.A
5. Sireef.P
6. VBLInject.UUG
7. Sienbot.ALE
8. Rimecud.A
9. Dynameriddc.A
10. Fynioski.A

April with a total of 35,558 cases saw an 86 percent increase in the total number of phishing attacks. Comparing this year’s figure to its last year equivalent shows that the number doubled. The spring and summer are usually when most attack peaks are recorded, and it appears that April set the tone for what’s to come this season.

Source: RSA Anti-Fraud Command Center
2 minutes on...
The promise of Windows 8
P14
Me and my job
Addressing policy for seamless mobile capability P15
Skills in demand
Security pros with infrastructure experience needed P15

NEWS BRIEFS

• Ontario received a record number of privacy complaints last year, according to the province’s privacy commissioner. Some 266 new complaints were opened, up 5.6 percent over the previous year.

The data, which came from the Ontario Information and Privacy Commissioner’s 2011 annual report, showed that Ontarians were most worried about who was seeing their information. Most of the complaints concerned information disclosure, with the vast majority most common addressing the way that organizations were securing individuals’ information.

The complaints were filed under the provincial and municipal Freedom of Information and Protection of Privacy acts. Roughly half of the complaints were filed under each law.

• The hacktivist group Anonymous published online the personal information of Canadian politicians as part of a protest over the treatment of student protesters in Montreal. The group stole the information of fans who bought tickets to the forthcoming Formula One race in the city.

• Google to pay
The Federal Communications Commission (FCC) in the United States settled with Google over its unauthorized collection of Wi-Fi data as part of its “Street View” project. The search giant must pay $25,000 for being uncooperative during the investigation. Google insists the collection was an accident. The company also faces a fine over its placement of cookies on Safari in order to bypass built-in protections.

Google’s collection of data (via Wi-Fi) was met with a privacy uproar.

The QUOTE

My first reaction was, ‘Wow, they did a lot.’”

– Chris Valasek, senior security research scientist at Covesity, on new export mitigation functionality in Windows 8, set for release later this year.

Debate
Sharing security data is the best way to raise the cost of entry and lower ROI for criminals and spies.

FOR
Open information sharing develops an intrinsic capacity for intelligence and sustainable security practices within the fabric of business itself, freeing us from an artificial reliance on the business model of any particular vendor. Just as true scientific progress is robbed of the ability to make unintended discoveries when data is held behind a paid curtain, we cheat ourselves of the providence of progress via pure research in the field. The nature of the “information age” leaves no business an island. Being less insecure than your competition is an illusion of competitive advantage. Individually, nobody knows all the pieces to the puzzle, while collectively we hold most of them. When a few organizations hold all the cards, government regulation is inevitable. Our failure to realize our obligation to share intelligence and take a collective stand is why the Cyber Intelligence Sharing and Protection Act (CISPA) is the regulation we deserve, not desire. We can either make efforts to change our approach to defense, or continue to let our misery be monetized.

AGAINST
Implementation of often-ignored basic countermeasures is a more effective way to protect critical information. The majority of recent, impactful security breaches could have been prevented by implementing these measures to protect information and systems considered critical to their respective organizations. These countermeasures, such as encryption of sensitive information in various formats and ongoing user-awareness training programs, are a few examples of universal best practices widely regarded as “the basics.” Every organization that conducts business on the internet is at risk, and threat agents will do the bare minimum to achieve their goals. Implementing basic countermeasures as a comprehensive approach to security will raise the bar for threat agents, increase their cost of doing business, and reduce their ROI. Basic security controls are usually effective enough to counter most threats. It is only when organizations have a handle on the basics can the full value of shared intelligence be realized.

THE STATS

206
Republicans in the House voted in April to approve CISPA: 42 Democrats voted no

61.25%
Scrap it

16.25%
Pass it

22.5%
Keep it, but ensure civil liberties are protected

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

THE SC MAGAZINE POLL
Do you support CISPA, which would allow the sharing of threat data?

THREAT OF THE MONTH

Crimeware packs

What is it?
Crimeware packs, also known as mass malware packs, are software toolkits that are designed to exploit vulnerabilities in order to steal information from unsuspecting victims who are usually infected via drive-by downloads.

How does it work?
Crimeware packs are installed or embedded in compromised websites. The software usually contains several exploits, varying from old to new.

Should I be worried?
Crimeware packs are widely available and some of the more popular ones can be obtained for free. There is no shortage of web application vulnerability scans, and there is no effective way to prevent it.

How can I prevent it?
Everyone should keep their software up to date and actively monitor patches with vulnerability scanning. Everyone should keep their software up to date and actively monitor patches with vulnerability scanning. Everyone should keep their software up to date and actively monitor patches with vulnerability scanning. Anti-virus solutions won’t detect zero-day malware, they do work well for detecting common threats. There is no shortage of web application vulnerability scans, and there is no effective way to prevent it.

– Marcus Cains, security researcher at Rapid7

S. 2151
(Secure IT), another cyber security bill, was introduced in March by Sen. John McCain, R-Ariz.

Source: news reports

• Anon

Our failure to realize our obligation to share intelligence and take a collective stand is why the Cyber Intelligence Sharing and Protection Act (CISPA) is the regulation we deserve, not desire. We can either make efforts to change our approach to defense, or continue to let our misery be monetized.

Source: news reports

• Anon

Every organization that conducts business on the internet is at risk, and threat agents will do the bare minimum to achieve their goals. Implementing basic countermeasures as a comprehensive approach to security will raise the bar for threat agents, increase their cost of doing business, and reduce their ROI. Basic security controls are usually effective enough to counter most threats. It is only when organizations have a handle on the basics can the full value of shared intelligence be realized.

Source: news reports

• Anon

There is no shortage of web application vulnerability scans, and there is no effective way to prevent it.

– Marcus Cains, security researcher at Rapid7

S. 2151
(Secure IT), another cyber security bill, was introduced in March by Sen. John McCain, R-Ariz.

Source: news reports

• Anon

What is it?
Crimeware packs, also known as mass malware packs, are software toolkits that are designed to exploit vulnerabilities in order to steal information from unsuspecting victims who are usually infected via drive-by downloads.

How does it work?
Crimeware packs are installed or embedded in compromised websites. The software usually contains several exploits, varying from old to new.

Should I be worried?
Crimeware packs are widely available and some of the more popular ones can be obtained for free. There is no shortage of web application vulnerability scans, and there is no effective way to prevent it.

How can I prevent it?
Everyone should keep their software up to date and actively monitor patches with vulnerability scanning. Although anti-virus solutions won’t detect zero-day malware, they do work well for detecting common threats. There is no shortage of web application vulnerability scans, and there is no effective way to prevent it.

– Marcus Cains, security researcher at Rapid7

S. 2151
(Secure IT), another cyber security bill, was introduced in March by Sen. John McCain, R-Ariz.

Source: news reports

• Anon

Every organization that conducts business on the internet is at risk, and threat agents will do the bare minimum to achieve their goals. Implementing basic countermeasures as a comprehensive approach to security will raise the bar for threat agents, increase their cost of doing business, and reduce their ROI. Basic security controls are usually effective enough to counter most threats. It is only when organizations have a handle on the basics can the full value of shared intelligence be realized.

Source: news reports

• Anon

There is no shortage of web application vulnerability scans, and there is no effective way to prevent it.

– Marcus Cains, security researcher at Rapid7

S. 2151
(Secure IT), another cyber security bill, was introduced in March by Sen. John McCain, R-Ariz.

Source: news reports
The promise of Windows 8

When the latest version of the most popular operating system (OS) 5 in the world is released in October, researchers in search of vulnerabilities will flock to the shiny, new platform. But creating exploits for Windows 8 may prove quite costly in terms of time, effort and skill.

Developed to be a multipurpose OS, the new iteration of Windows will run on desktops, tablets and other mobile devices. The new M etro-style interface, designed to be cleaner and more compatible with touch-screen devices, will turn heads, but the work done under the hood in terms of security appears to be equally impressive.

According to market researcher N eWDA applications, Windows is the most-used OS on the planet, running on more than 90 percent of computers and is thus the basis of malware authors’ attention. M icrosoft security has come a long way since XP, and the enhancements made to Windows 8 confirm this evolution, say experts.

Research conducted by Chris Valasek, senior security scientist for Coverity, a San Francisco-based software security company, says the most notable changes include a new App Container for the upcoming Windows 8 App Store, which will limit actions certain applications can perform. In addition, the OS will feature enhanced exploit mitigation technology to combat memory issues like buffer and heap overflows.

“If I was writing an exploit I would not want to do it for Windows 8,” Valasek said. “There are a lot of hurdles to overcome when writing an exploit that would target this operating system.”

While the improvements may not be revolutionary, Valasek said they are proof that M icrosoft has realized the security problem can’t be solved overnight and is doing its best to protect end-users.

The computing giant’s progress comes at a time when its main competitor, A pple, is under fire for its seeming inattention to security. In April, the Flashback trojan hijacked nearly 700,000 computers worldwide through a java vulnerability. Although Oracle released a patch in February, it took A pple nearly two months to ship its own fix. Although progress with security is evident, Chester W iniarski, senior security adviser at British anti-virus firm Sophos, acknowledges the Windows 8 improvements, but they shouldn’t be enough to get users immediately off Windows 7.

“(Windows 8 is) making it a little harder for the bad guys, making them go the long way, but I don’t know if it results in your being safer,” he said. — Marcus Colón

92% share of desktop OS market that Windows maintains

– Net Applications

The University of Washington took top honors at NCCDC.

A team from the University of Washington won top honors at NCCDC.

The promise of Windows 8

When the latest version of the most popular operating system (OS) 5 in the world is released in October, researchers in search of vulnerabilities will flock to the shiny, new platform. But creating exploits for Windows 8 may prove quite costly in terms of time, effort and skill.

Developed to be a multipurpose OS, the new iteration of Windows will run on desktops, tablets and other mobile devices. The new M etro-style interface, designed to be cleaner and more compatible with touch-screen devices, will turn heads, but the work done under the hood in terms of security appears to be equally impressive.

According to market researcher N eWDA applications, Windows is the most-used OS on the planet, running on more than 90 percent of computers and is thus the basis of malware authors’ attention. M icrosoft security has come a long way since XP, and the enhancements made to Windows 8 confirm this evolution, say experts.

Research conducted by Chris Valasek, senior security scientist for Coverity, a San Francisco-based software security company, says the most notable changes include a new App Container for the upcoming Windows 8 App Store, which will limit actions certain applications can perform. In addition, the OS will feature enhanced exploit mitigation technology to combat memory issues like buffer and heap overflows.

“If I was writing an exploit I would not want to do it for Windows 8,” Valasek said. “There are a lot of hurdles to overcome when writing an exploit that would target this operating system.”

While the improvements may not be revolutionary, Valasek said they are proof that M icrosoft has realized the security problem can’t be solved overnight and is doing its best to protect end-users.

The computing giant’s progress comes at a time when its main competitor, A pple, is under fire for its seeming inattention to security. In April, the Flashback trojan hijacked nearly 700,000 computers worldwide through a java vulnerability. Although Oracle released a patch in February, it took A pple nearly two months to ship its own fix. Although progress with security is evident, Chester W iniarski, senior security adviser at British anti-virus firm Sophos, acknowledges the Windows 8 improvements, but they shouldn’t be enough to get users immediately off Windows 7.

“(Windows 8 is) making it a little harder for the bad guys, making them go the long way, but I don’t know if it results in your being safer,” he said. — Marcus Colón

92% share of desktop OS market that Windows maintains

– Net Applications

The University of Washington took top honors at NCCDC.

A team from the University of Washington won top honors at NCCDC.

The promise of Windows 8

When the latest version of the most popular operating system (OS) 5 in the world is released in October, researchers in search of vulnerabilities will flock to the shiny, new platform. But creating exploits for Windows 8 may prove quite costly in terms of time, effort and skill.

Developed to be a multipurpose OS, the new iteration of Windows will run on desktops, tablets and other mobile devices. The new M etro-style interface, designed to be cleaner and more compatible with touch-screen devices, will turn heads, but the work done under the hood in terms of security appears to be equally impressive.

According to market researcher N eWDA applications, Windows is the most-used OS on the planet, running on more than 90 percent of computers and is thus the basis of malware authors’ attention. M icrosoft security has come a long way since XP, and the enhancements made to Windows 8 confirm this evolution, say experts.

Research conducted by Chris Valasek, senior security scientist for Coverity, a San Francisco-based software security company, says the most notable changes include a new App Container for the upcoming Windows 8 App Store, which will limit actions certain applications can perform. In addition, the OS will feature enhanced exploit mitigation technology to combat memory issues like buffer and heap overflows.

“If I was writing an exploit I would not want to do it for Windows 8,” Valasek said. “There are a lot of hurdles to overcome when writing an exploit that would target this operating system.”

While the improvements may not be revolutionary, Valasek said they are proof that M icrosoft has realized the security problem can’t be solved overnight and is doing its best to protect end-users.

The computing giant’s progress comes at a time when its main competitor, A pple, is under fire for its seeming inattention to security. In April, the Flashback trojan hijacked nearly 700,000 computers worldwide through a java vulnerability. Although Oracle released a patch in February, it took A pple nearly two months to ship its own fix. Although progress with security is evident, Chester W iniarski, senior security adviser at British anti-virus firm Sophos, acknowledges the Windows 8 improvements, but they shouldn’t be enough to get users immediately off Windows 7.

“(Windows 8 is) making it a little harder for the bad guys, making them go the long way, but I don’t know if it results in your being safer,” he said. — Marcus Colón

92% share of desktop OS market that Windows maintains

– Net Applications

The University of Washington took top honors at NCCDC.

A team from the University of Washington won top honors at NCCDC.
Let’s educate our lawmakers

Eugene Fredriksen
CSO, Tyco International

Over the past few years, numerous bills on cyber security have been introduced and gone nowhere in Congress. That’s about to change. The House leadership announced during “Cyber Security Week” in April that it approved four bills. The Senate is currently attempting to resolve largely partisan differences among competing cyber bills. Chances of reaching a compromise are probably 50-50.

The good news is that Congress is beginning to take the problem seriously. The bad news is that, with a few exceptions, federal lawmakers mostly think we now inhabit. We owe it to ourselves and our industry to address these core issues as part of their day jobs substantially upgrade the education program for our elected officials. This is a call to action. Become educated. Express your concerns. Get involved. Contact your representatives directly or work through professional organizations, such as the Internet Security Alliance. Share your expertise, experiences and concerns with those crafting the laws with which we will all have to comply. The only certainty in this process is that we will all have to live with final legislation for the coming years. Let’s get involved and influence the future of our industry.

The always-on resource for IT professionals

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

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

With saboteurs plundering organizations of coveted assets, it’s time to fight back, says Joel Yonts, CISO of a Fortune 500 merchant. Dan Kaplan reports.

J oel Yonts, the CISO of a Fortune 500 automotive supply company, isn’t pleased with many of his peers. Their complacency and timidity around security is widening the chasm between victory and defeat by an ever-growing margin, and simply put, the losses really are piling up.

In security, where the threats evolve on an almost daily basis, most organizations – even ones operating the most proficient networks – seem content with the traditional perimeter-based, compliance-focused approach of battling the enemy. Yonts says. Such block-and-tackle tactics, as they are known among security pros, may work against the so-called low-hanging-fruit threats – things like SQL injections and common trojans – but they hit a brick wall when it comes to dealing with more sophisticated weaponry, like espionage malware.

“I am tired of [hearing], ‘We are defending at the gate and we are winning’,” says Yonts, 40, the CISO since 2006. “No, we’re just letting the attackers attack us as many times as they want until they get in.” He blames this inherent defect on an industry where security programs largely have been built by the guidance of audit firms, which place heavy emphasis on meeting compliance mandates, such as Sarbanes-Oxley and apply a good deal of weight to guarding against the insider threat, often overlooking today’s advanced adversary.

Meanwhile, networks are getting owned with regularity by well-funded and well-trained assailants, who use their deep pockets and slick skills to quietly burrow in, establish a foothold and then purge sensitive data. In many cases, the victim organization doesn’t learn about the intrusion for weeks, months, or even years – and even then, a third party is the entity that usually notifies them.

“They’re bleeding data,” Yonts says of the targeted firms. “They can be happy with their compliance scores, but they’re bleeding data.” Worst of all, these enterprises are operating under a false sense of security. “If they’ll totally downplay a compromised PC because the connection between one compromised PC turning into data exfiltration is not something people are living with,” he says.

As evidence, Kroll Adivisory Solutions’ recent report, “HIMSS Analytics Report: Security of Patient Data,” which examined the health care industry in particular, found that despite increasing rates of compliance, the number of organizations reporting breaches jumped from 13 percent in 2008 to 27 percent last year.

It’s become a common refrain that security doesn’t equal compliance, yet many practitioners remain asleep at the switch. Yonts is not alone in his sentiment. Yonts is not alone in his sentiment.

According to Shawn Henry, the FBI’s former top cyber cop, got quite a bit of backlash when, upon announcing his retirement, took to the media to proclaim that the nation is on the losing end of the war on hackers.

“I don’t know that we can ever get ahead of this right now with the current state of architecture and attribution,” says Henry, now president of services at security start-up CrowdStrike.

“Defending at the gate and we are winning”

“As evidence, Kroll Adivisory Solutions’ recent report, “HIMSS Analytics Report: Security of Patient Data,” which examined the health care industry in particular, found that despite increasing rates of compliance, the number of organizations reporting breaches jumped from 13 percent in 2008 to 27 percent last year.

It’s become a common refrain that security doesn’t equal compliance, yet many practitioners remain asleep at the switch. Yonts is not alone in his sentiment.

For example, the company takes great stock in its email security and awareness training. Both speak to the common hacker ploy of spreading spam or inserting malware into a target network by tricking an employee at the company to click on an email attachment that looks legitimate, but isn’t.

But, when trying to counter the more advanced risks is when his fourth and fifth tenets kick in: incident response and attribution. These pillars are especially important for Yonts’ business, which can easily become a victim of the trusted relationships it has formed with partner organizations.

“[If attackers] were able to compromise one of my vendors and implant malicious code in my data, it would be very hard for me to detect it,” Yonts says. “If another on打听, you’ll have some vulnerability left and some attacks will get through.”

Instead, within the private sector, organizations can retaliate in other ways, including sharing information about the opponent or driving the hackers’ costs up by making successful attacks much more difficult to accomplish.

“…companies have to think more like they are spies.”

– David Burg, PricewaterhouseCoopers
Cyber strategy

Don’t underestimate the significance of that last sentence. In a time where more security pros are accepting the realization that network compromise is a part of doing business, Yonts understands this isn’t a death sentence. In fact, his own company sustained a breach in 2008 and was forced to notify 56,000 customers that their financial data was exposed by a hack. But, the incident could have been worse.

“You’re not talking about 56,000 customers, you’re talking about a five-sided building in Arlington County, Va. But, Yonts says he has come up with the next best thing: hitting the attackers where it hurts – in the wallet. He calls this final pillar “attrition.”

The previous step – incident response – speaks to quickly identifying and shutting down a successful infiltration before it can do any sizeable damage. Combine that with gathering evidence about the attacker to share with anti-virus companies and law enforcement, and Yonts and his team are trying to effectively eradicate the value proposition for the criminal.

To share threat intelligence data, Yonts leverages the bonds he has formed in the research community thanks to his role as chief scientist and founder of M Alcious Streams, a side project that analyzes malicious code and hacker techniques. Yonts strongly believes in collaboration. Wether his company is hit by an attack with the goal to steal data center space in order to launch spam or distribute undetected-of-service (DDoS) attacks, all the way to more sophisticated assaults designed to pillicate credit card numbers or intellectual property, he will share that data with the pertinent parties.

“Suddenly every AV company has all the samples,” he says. “They have automated systems. Suddenly everyone in the world is protected within a couple of hours.”

The next step is to prepare a more formal version of the attack to be shared with law enforcement, Yonts forensic investigation team is trained in compiling evidence that is “completely admissible” in court. That may not always mean providing the suspected names of the responsible parties, but sometimes clues, such as offending IP addresses, can go a long way to bring charges against someone, especially when combined with an investigation already underway by the FBI or a related agency.

“We are not seeing anyone going truly offensive in terms of hacking back in the commercial space,” Burg says. “H however, companies are starting to think aggressively.”

Some organizations are turning to tactics like sandboxing, honeypots and decoy/dummy data to throw an attacker off the scent or allow them to be traced. “We certainly take the advantage to socially engineer the attacker back,” Yonts says. “We’ll try to attack their system, but to confuse and disorient them.”

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defenders,” he says. “They trum of operations when you compare the threat, he says.

Amit’s response plan is not unlike that of Yonts – understand what one needs to do to current defende
The intelligence community in Canada is diverse and widespread...and lacks oversight. Danny Bradbury explores the implications.

In a September 2006 report on Canada’s participation in the rendition and torture of Maher Arar, a Canadian engineer held in a Syrian jail, Justice Dennis O’Connor identified several agencies that cooperate regularly with the Royal Canadian Mounted Police (RCMP) on national security issues. These include the usual suspects, such as CSIS and CSEC. But there also were a broad variety of other agencies. For example, the Integrated Threat Assessment Centre (ITAC), which was created in 2004, identifies threats to Canadian national security both domestically and internationally.

Others are tasked with policing the physical borders, such as the Canada Border Services Agency (CBSA) and Transport Canada, which manages the no-fly list. There are more. The Department of Finance and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) hold key national security responsibilities, as do the Department of Foreign Affairs and International Trade (DFAIT). The Department of Fisheries and Oceans, the Privy Council Office, Health Canada, and Public Safety and Emergency Preparedness Canada are all key national security players, as are the Department of National Defense (DND) and the Canadian Forces.

SIRC’s concerns about the level and depth of integration between CSIS and other agencies appear valid. CSIS works closely with several federal government departments and agencies, including the DFAIT, the DND, the CBSA, the National Research Council and the Canadian Nuclear Safety Commission. It is also permitted to work with any federal, provincial or international governmental organization with the permission of the minister of public safety, although SIRC must be notified.

All of this becomes more problematic due to the lack of sufficient complaint mechanisms surrounding national security activities in Canada, says Roch Tassé, national coordinator at the International Civil Liberties Monitoring Group. “CSIS already has a narrow complaint mechanism, and when you come to integrated operations there is no point of entry,” he says. “You never know who has been abused by which agency, and there is no place to run independent reviews. We have identified at least a dozen agencies involved in national security operations and none of them have an official complaint mechanism.”

At least CSIS has a grievance process, even if it is relatively limited and now governed by an agency with limited powers. Other agencies have no such process at all. This, along with sweeping powers, makes them extremely powerful with little to no accountability, says Tassé, who offers the border service as an example. “The CBSA has become a major player in national security issues in Canada,” he says. “They’re enforcing supervision of people under security certificates. They’re responsible for expulsions over the border. And yet there’s no complaint or review mechanism, even an integrated one. They operate in total impunity.”

This becomes even more troubling in the context of the North American Security Perimeter Agreement, which was released in December because it extends the intimate integration among national security agencies over the border. The agreement calls for more informal information sharing between Canada and the United States. “So even with a strong Canadian oversight mechanism, it would become impossible to investigate,” says Tassé.

Further consequences

There are other concerns too, says Dave Millier, CEO of SentryMetrics, a provider of managed security services based in Toronto. He points to recent worries over large telecommunications contracts awarded by Canadian firms to Chinese vendor Huawei Technologies. U.S. security officials criticised Canada for letting Huawei sell telecommunications products to its companies on the grounds that the firm could tamper with equipment, providing digital backdoors for espionage purposes. Telus, which is a large customer of Huawei’s, has signed a $250 million contract with the Department of National Defence.
operations involving the RCMP. And where requested by the governor in council, ICRA should be able to expand its scope beyond the scope of the RCMP to independently review other national security agencies, thus providing insight into the operations of agencies that currently have no review mechanism.

The Public Safety Commission of Canada endorsed the O’Connor report, and in the fall of 2009, the majority of members in Parliament voted to approve the recommendations.

Lack of accountability
While others call for a single set of overseers for the intelligence community, Rafal Rohozinski wants a more granular approach that promotes cyber security. The founder of SecDev, a security consulting company in Ottawa that advises on operations and security policy, says he desires a more sophisticated approach altogether. Cyber security issues have evolved so quickly that they should be separated out in the context of intelligence operations, Rohozinski says.

“Cyber security and intelligence were lumped together,” he says. “Now, things are complex enough that things need to be segregated.”

The lack of accountability in the intelligence community is made more acute by a lack of parliamentary openness, he adds. “It’s easy to demonstrate that Canadian parliamentary oversight is quite weak,” he says. For example, the North American “security perimeter” — a proposed agreement that would facilitate the egress of goods and people across the shared border between Canada and the United States — will be implemented largely through regulations, which makes it impossible for individual measures to be debated in Parliament. “It’s executive oversight, and for a number of functional and oversight reasons we don’t just want security reporting to the executive,” Leuprecht says.

And so, the dance between intelligence agencies and overseers continues. The intelligence community will always believe that there is too much oversight, while civil liberties groups and some academics will always believe that they are not given enough information. As the level of information sharing among different agencies in the national security community continues, these tensions will continue to rise.

### National security

### Alphabet soup: Intelligence agencies in Canada

<table>
<thead>
<tr>
<th>Name of agency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canadian Security Intelligence Service (CSIS)</td>
<td>Canada’s national intelligence service responsible for collecting, analyzing, reporting and disseminating intelligence on threats to Canada’s national security and conducting operations, covert and overt, within Canada and abroad.</td>
</tr>
<tr>
<td>Communications Security Establishment Canada (CSEC)</td>
<td>The government’s national cryptologic agency, administered under the Department of National Defence (DND), it is charged with keeping track of foreign signals intelligence (SIGINT), and protecting Canadian government electronic information and communication networks.</td>
</tr>
<tr>
<td>Intelligence Branch of Canadian Forces</td>
<td>The personnel branch of the Canadian Forces (CF) that is concerned with providing relevant and correct information to enable commanders to make decisions.</td>
</tr>
<tr>
<td>Criminal Intelligence Service Canada (CISC)</td>
<td>An interagency organization designed to coordinate and share criminal intelligence amongst member police forces.</td>
</tr>
<tr>
<td>Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)</td>
<td>Gathers, analyzes, assesses and discloses financial intelligence.</td>
</tr>
<tr>
<td>Royal Canadian Mounted Police (RCMP)</td>
<td>The national police force.</td>
</tr>
<tr>
<td>Canada Border Services Agency (CBSA)</td>
<td>A federal law enforcement agency responsible for border and immigration enforcement and customs services.</td>
</tr>
<tr>
<td>Chief of Defence Intelligence (Canada) (CDI)</td>
<td>An intelligence agency, part of the broader security and intelligence community, comprised of several departments and agencies that collect and analyze intelligence on issues of concern to Canada, and also manages DND/CF national/international intelligence partnerships.</td>
</tr>
</tbody>
</table>
Criminals are finding that social networking sites like Facebook are rich in data, reports Ryan Goldberg.

Hugh Thompson, who is the program committee chairman of the annual RSA Conference, also teaches a class on software security at Columbia University in New York. Two years ago, a few of his students looked into an online forum in which software developers share troubleshooting advice. The students wrote a basic source code scanner that connected login names on this forum to LinkedIn and Twitter, thus identifying these developers and extrapolating which companies had vulnerabilities in their systems.

Their motive was harmless, but the students showed how hackers could execute this. “The data could be fused,” Thompson says.

The lynchpin, of course, was social media, as content available on these popular user-generated sites was wielded to mine data to target a single company, says Thompson. “The data could be fused,” Thompson says.

Last November, “socialbots,” which researchers from the University of British Columbia at Vancouver released onto Facebook, made off with 250 gigabytes of personal information belonging to thousands of users. Or take the case of the GhostNet Chinese spy ring, uncovered by University of Toronto researchers in 2010, where malware networks were organized and operated through Web 2.0 programs, such as Twitter and Google Groups, to steal sensitive documents from the Dalai Lama, governments and corporations.

In the past, email provided one doorway for phishing attacks. With social networks, phishing now comes from several routes. The growth of “personalization tools,” as Thompson calls it, drives the cost of creating one more personalized email to zero.

This data can be used explicitly and inferentially. Thompson describes an IT industry analyst who estimates the sales figures of small companies. Since these figures aren’t public, the analyst searches LinkedIn for former salespeople of these companies, many of whom include in their profiles the sales growth they drove during their time at that company. Privacy and social networks are inherently at cross purposes, and security factors into this equation. The more information one shares, the more they and their friends get out of it – in an endless feedback loop. The business model of online social networks depends on this for advertising revenues.

“Relationships in the social fabric have become automated,” says Joe Gofflied, the CEO and president of Sensage, a data warehouse software provider. “To me, that is a very impactful trend.”

Last November, “socialbots,” which researchers from the University of British Columbia at Vancouver released onto Facebook, made off with 250 gigabytes of personal information belonging to thousands of users. Or take the case of the GhostNet Chinese spy ring, uncovered by University of Toronto researchers in 2010, where malware networks were organized and operated through Web 2.0 programs, such as Twitter and Google Groups, to steal sensitive documents from the Dalai Lama, governments and corporations.

In the past, email provided one doorway for phishing attacks. With social networks, phishing now comes from several routes. The growth of “personalization tools,” as Thompson calls it, drives the cost of creating one more personalized email to zero.

This data can be used explicitly and inferentially. Thompson describes an IT industry analyst who estimates the sales figures of small companies. Since these figures aren’t public, the analyst searches LinkedIn for former salespeople of these companies, many of whom include in their profiles the sales growth they drove during their time at that company. Privacy and social networks are inherently at cross purposes, and security factors into this equation. The more information one shares, the more they and their friends get out of it – in an endless feedback loop. The business model of online social networks depends on this for advertising revenues.

“Relationships in the social fabric have become automated,” says Joe Gofflied, the CEO and president of Sensage, a data warehouse software provider. “To me, that is a very impactful trend.”

Last November, “socialbots,” which researchers from the University of British Columbia at Vancouver released onto Facebook, made off with 250 gigabytes of personal information belonging to thousands of users. Or take the case of the GhostNet Chinese spy ring, uncovered by University of Toronto researchers in 2010, where malware networks were organized and operated through Web 2.0 programs, such as Twitter and Google Groups, to steal sensitive documents from the Dalai Lama, governments and corporations.

In the past, email provided one doorway for phishing attacks. With social networks, phishing now comes from several routes. The growth of “personalization tools,” as Thompson calls it, drives the cost of creating one more personalized email to zero.

This data can be used explicitly and inferentially. Thompson describes an IT industry analyst who estimates the sales figures of small companies. Since these figures aren’t public, the analyst searches LinkedIn for former salespeople of these companies, many of whom include in their profiles the sales growth they drove during their time at that company. Privacy and social networks are inherently at cross purposes, and security factors into this equation. The more information one shares, the more they and their friends get out of it – in an endless feedback loop. The business model of online social networks depends on this for advertising revenues.

“Relationships in the social fabric have become automated,” says Joe Gofflied, the CEO and president of Sensage, a data warehouse software provider. “To me, that is a very impactful trend.”

Last November, “socialbots,” which researchers from the University of British Columbia at Vancouver released onto Facebook, made off with 250 gigabytes of personal information belonging to thousands of users. Or take the case of the GhostNet Chinese spy ring, uncovered by University of Toronto researchers in 2010, where malware networks were organized and operated through Web 2.0 programs, such as Twitter and Google Groups, to steal sensitive documents from the Dalai Lama, governments and corporations.

In the past, email provided one doorway for phishing attacks. With social networks, phishing now comes from several routes. The growth of “personalization tools,” as Thompson calls it, drives the cost of creating one more personalized email to zero.

This data can be used explicitly and inferentially. Thompson describes an IT industry analyst who estimates the sales figures of small companies. Since these figures aren’t public, the analyst searches LinkedIn for former salespeople of these companies, many of whom include in their profiles the sales growth they drove during their time at that company. Privacy and social networks are inherently at cross purposes, and security factors into this equation. The more information one shares, the more they and their friends get out of it – in an endless feedback loop. The business model of online social networks depends on this for advertising revenues.

“Relationships in the social fabric have become automated,” says Joe Gofflied, the CEO and president of Sensage, a data warehouse software provider. “To me, that is a very impactful trend.”
Managing policy and risk requires sophisticated tools

We usually focus on the tools of our trade and occasionally forget that the foundations of a secure network enterprise are wrapped up in our policies. It is from our security guidelines that we derive the configurations for interconnecting network devices, such as routers, switches and firewalls. We configure servers and endpoint devices, such as workstations and mobile devices, based on our policies.

Be that as it may, policy is the foundation for the practical implementation of enterprise security. But where do we get our strategies? In a well-managed network, those policies are the result of a close examination and analysis of the risks inherent in the network. The foundation is a multilayered function derived from threat, vulnerability and impact. Add in a healthy dose of countermeasures to mitigate the risk and one has a picture of the security in the enterprise environment.

Risk measurement and quantification in a dynamically changing environment requires tools that can take lots of inputs from sensors around the enterprise, measure threats from a variety of sources, balance those metrics against the criticality of devices and security domains on the network and keep track of the interactions. Typically, we have treated these two functions as separate groups. This year, we have taken them together because more and more we are seeing both functions in the same device.

These tools are not for the faint-hearted. They can be complex to configure, they are expensive and need careful feeding as the network changes, an inevitability that we all will accept as the way things are in our field.

Th at said, though, these may be among the most valuable tools in your arsenal. These applications, software and services are valuable because they enable other tools to work at the peak of their efficiencies and manage the outputs and configurations of other devices.

This month, Mike Stephenson and Mike Lipinski did the honors in the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

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 15408) 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 based on the judgment and interpretation of the tester and are validated by the technology editor.

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

What the stars mean

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

★★★★ Outstanding. An “A” on the product’s report card.
★★★★★ Carries all basic functions very well. A “B” on the product’s report card.
★★★★ Carries 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.

What the recognition means

Best Buy goes to products the SC Lab rates as outstanding. Recommended means the product has shown 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.

For a vulnerability to be exploited there needs to be a threat, and the threat agent must have access to the vulnerability. That access is called reachability. So the notion of reachability is inherent in the notion of vulnerability. The issue is complicated a bit by the fact that, today, attacks often are not simple one-off exploits. They may be chained exploits within the enterprise itself or they may require the use of a pivot (a vulnerable device that can be compromised and then used, in turn, to compromise other devices that trust it). That means that analysis – and subsequent management – of vulnerabilities is not a simple process.

Sometimes, it is easier and more efficacious to manage threats. In that case, we usually place some sort of countermeasure between the threat and exploitable vulnerabilities in general. The notion of vulnerability is that both threats and vulnerabilities are an ever-shifting landscape and therefore, challenging to manage. That is what the tools that we are reviewing come into the picture. They handle this dynamic environment far more efficiently than can a human administrator.

Compliance is the third leg of the GRC stool. It is the elephant in the room. Compliance is expensive and complicated, but necessary. While files are not particularly common yet, the penalties for being out of compliance with regulatory requirements can be significant. More important, a case of ID theft traceable to an organization’s negligence in maintaining compliance can result in lawsuits.

Managing GRC means controlling both risks and the configurations of the devices meant to implement policy as a countermeasure to risk. It is a basic tenet of information assurance that one must have a technical way to enforce policies. Simply telling people that they need to follow certain password rules, for example, is not a reliable way to implement that policy. The system needs to have a way to enforce the plan. Policy management tools do that for you.

W hen one combines risk and policy management into a single tool, the best of both worlds is available. One analyzes the ever-changing risk landscape and then adjusts appropriate devices in the enterprise to mitigate the discovered risks.

Clearly, we don’t usually behave in that old-school manner, but GRC management done manually is not for everyone. If yours fits into any of the many categories of organizations that must be compliant with the multitude of regulatory requirements that bedevil – and protect – us, the tools we look at this month are critical to success, says Peter Stephenson.

Erroratum: Last month, we mis-reported the pricing for WetStone Technology’s US-LATT product. The correct pricing is $1,495 (includes one-year free product maintenance); maintenance: $299/year after the first year. We apologize for the error.
## Specifications for risk & policy management tools

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Agiliance RiskVision v6.0SP2</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>AlgoSec Security Management Suite v6.2</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Citirus ONE v3.4</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>eGestalt Technologies SecureGRC Enterprise v11</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>FireMon Security Manager with Policy Planner v6.0 and Risk Analyzer v1.1</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>LockPath Keylight Platform v2.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Lumension Risk Manager v4.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>McAfee Total Protection for Compliance v7</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>MetricStream Risk Management Solution and Policy Management Solution v6.0</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Modulo Security Risk Manager v7.6</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>NetIQ Secure Configuration Manager v5.8</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>NetWrix Change Reporter Suite v2.0</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>New Net Technologies NNT Change Tracker Enterprise v5</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>RedSeal v5.0</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>RSA Archer eGRC Suite v5.1.4</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Rsam eGRC Platform v7.5</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Skybox View Enterprise Suite v6.0</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SolarWinds Network Configuration Manager v7.0</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Symantec Control Compliance Suite v11</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Tripwire Enterprise v8.1</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Tufin Security Suite vR12-1</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Viewfinity Privilege Management v3.8</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
Agiliance RiskVision v6.0 SP2

A
giliance RiskVision is a purpose-built G.R.C. solution that brings together threat and vulnerability data, security configuration data, compliance and risk assessment information into a single, task-driven console. It correlates this data against its “business-criticality aware” asset database, as well as its multi-regulatory compliance framework of 50 standards and policies, providing organizations with an aggregated view of their risk and compliance posture.

The solution is delivered as a software offering or as an “in the cloud” hosted offering. The requirements for deployment include: MS W indows Server 2003 or 2008, MySQL 5.5 or Oracle Database 11g, web browser (IE 6.0, 7.0, 8.0 or 9.0 or Firefox 3.0 or 4.0), Adobe Flash v10 or higher. The typical deployment takes 30 to 60 days on average.

RiskVision comes as a single platform with multiple modules that you can activate via licensing. The available modules include compliance manager, enterprise risk, vendor risk, threat and vulnerability, policy and incident manager. RiskVision combines top-down business controls with bottom-up operational data for real-time, security risk management. The user interface is cleanly done with web-based access that employs role-based authentication to deliver the customizable landing page determined by the user’s level of access. Tabbed-based navigation with multiple panes for data and graphic displays puts a lot of information on the screen while making it simple to navigate between modules, tabs and resources.

There is a lot of prepopulated content for policy, assessment, controls and reporting. RiskVision supports continuous import/export of data using prebuilt templates from MS Word, Excel and extensible markup language. RiskVision has a web-service, open-integration platform and toolkit, plus an extensive library of 35 purpose-built connectors to enable real-time integration with all types of products for identifying, policy, zero-day threat, vulnerability, event, technological, incident, data leakage prevention, ticketing, patch management, reporting, analytics and business intelligence.

RiskVision covers all aspects of risk management by providing assessments and policy, configuration and vulnerability management. This tool delivers on the compliance side of risk, as well as the IT risk management portion for a full-featured offering. Bundled with the risk options is a closed-loop remediation solution via its own integrated ticketing and exception processes. One also has the ability to integrate with most third-party ticketing and patch management solutions. An integrated workflow tool allows for quick programming of action items based on various risk criteria.

Reporting and dashboarding is very strong. RiskVision supports performance and risk metrics – key performance indicator (K PI)/key risk indicator (K R I) – risk registers, risk catalogue (including custom operational and business risks), and more than 300 rich, audit-ready dashboards and reports. The level of integration between the modules allows RiskVision to define a causal chain of a business-level risk down to its supporting assets and individual controls.

RiskVision is a complete risk offering, delivering on compliance, business risk and IT risk management.

Citicus ONE release 3.4

C

iticus O N E uses web-based data collection forms – including asset criticality assessments and risk scorecards underpinned by detailed threat and vulnerability checklists – to ensure that objective and consistent data is recording identifying risks to business applications, IT infrastructure and outsourced services.

Citicus O N E is available as both an installable software product and as an in-the-cloud-hosted service. The on-premise solution is supported on M S W indows Server 2003 or above, M S SQL Server 2005 or 2008, and requires IIS and X ML Core Services.

Citicus O N E supports a proportionate risk management process using a phased approach to risk management. Phase 1 is the criticality assessment, where one will assess the criticality of each of the evaluation targets. Phase 2 evaluates the risk posed by critical targets of evaluation by completing risk scorecards using a risk workshop. Phase 3 focuses on the owners of the tasks completing scorecards and remediation plans.

This is an assessment-based risk tool that uses a balanced risk scorecard methodology. The tool is used to create evaluations for targets, such as business applications, IT infrastructure, suppliers and site-type targets. Assessments are delivered automatically or in scheduled fashions. The risk metrics used are based on five determinants: control weakness, criticality, level of threat, business impact and special circumstances. Risk levels are tunable for one’s specific environment. Citicus One comes with some built-in control frameworks supporting ISO27001, PCI-DSS, Information Security Forum (ISF) Standard of Good Practice (SoGPr) and COBIT.

Assessments deliver evaluation results that create individual ‘issues’ or ‘action plans’ for follow-up or remediation activities. Citicus O N E will help users link the issues with action items to establish the required control improvements to remediate or manage risk. Interdependencies among assets can be recorded so that risk dependencies can be tracked. There is a workflow/remediation capability under the issues section to assist with this effort.

The dashboard that consolidates the output from the evaluation effort provides a clean visual to non-technical asset owners. It is able to track and associate a risk to specific incident.

Strengths: Dependency risk maps detail the risk flow/remediation capability under the issues section to assist with this effort. The tool has a visual into their overall risk score, a graphical displaying a summary of the five determinate risk factors, and a helpful scatter diagram summarizing risk drivers by criticality. Dashboard and reporting is role-based and integrated with Active Directory or CA SiteMinder for user management. Inter-reporting is provided at multiple levels from “owners” of individual assets on the ground to top management who require an overview of risk and compliance for a business unit or the entire enterprise. Reports include dashboards, risk and compliance league tables, heat maps, trend reports and risk dependency maps.

The documentation is integrated with the software and is efficiently laid out. Standard eight-hours-a-day/five-days-a-week support is included in the first year price and costs 18 percent thereafter. There are no optional levels of support available beyond standard.
eGestalt Technologies
SecureGRC Enterprise

SecureGRC is a cloud-based automated IT security and compliance management solution. SecureGRC supports both a security-centric and full-blown IT-GRC platform. The offering comes complete with an easy-to-use compliance-management framework, context-based inference engines, alert processing and easy-to-use logging and monitoring solution. The tool features easy-to-adopt and ready-to-use compliance management frameworks as well as context-based inference engines. In addition, SecureGRC features alert processing along with logging and monitoring capabilities.

Available in Enterprise and SB (small business) editions, SecureGRC is a cloud-based, Saas-delivered security and risk assessment, auditing and remediation application. It is generally sold through its reseller channels. All data is stored in a Saas 70 Title II secure data center and no electronic record information is removed from a client site. SecureGRC contains ready-to-use compliance control kits for PCI-DSS 1.2, ISO 27001/27002, COBIT, Sarbanes Oxley, HIPAA/A/HITECH , Gramm-Leach-Bliley Act, and other country-specific frameworks.

The tool provides real-time status on the current state of security and compliance and then offers a checklist of questions that guides the process along, asking for proof of documentation to fulfill the compliance request.

No prior knowledge of any particular compliance regulation is necessary in order to use SecureGRC. As a hosted solution, the interface is a web browser. Older browsers are not supported. The user interface is fairly easy to decipher with pull-down selections for customized assessments, controls, risk ratings and more. Users simply follow the application's list of instructions, upload the required documents and the system in the end will generate a report that can be presented to auditors to prove compliance. There is a substantial amount of prepopulated content around the regulatory and compliance standards listed above. Setup requires one to establish user accounts and provision them based on required levels of access. One then selects the templates needed for creating assessments from the list, customizes as necessary and publishes the assessment. Emails are sent to the users with their credentials for accessing the assessment questions. There is a closed-loop review process where the auditor can ask for additional information to complete the assessment. One nice process finishes, the compliance reports are generated. One doesn't have to be highly technical to use the tool. There is a sensible knowledge base built in that dynamically displays key information relating to the areas one is clicking on.

Documentation is built into the product with a series of drill-down mouse clicks to get to help-related information on a specific topic. Support is delivered via channel partners so fees will vary. If the next version can add in asset management and IT risk correlation, this would be a great product to look at if you are looking for a hosted GRC solution.

LockPath Keylight Platform v2.3

LockPath’s Keylight is a family of applications that manages enterprise risk and demonstrates compliance while providing visibility into corporate risk and security controls. Keylight provides a ready-to-use toolkit that unifies and correlates any amount of security content. It exposes threats and vulnerabilities detected throughout the organization by tracking and recording key information about secured assets and creating an iron-clad audit history.

The platform is offered as either an on-premise or cloud-based deployment option. O n-premise requirements include M S Server 2008 x64 or higher, M S SQL Server 2008 R 2 x64 or higher, and .NET Framework v4.0 with IIS 7.5 and Windows 50 K v70. The product deploys quickly and we were told that typical deployments get to an audit-ready point at about 30 days on average.

The platform consists of several “applications” that are all fully integrated under a single user interface. Applications are simply added through subsequent licensing. The applications consist of Compliance M anager, Threat M anager, Vendor M anager, Incident M anager, Risk M anager and Business Contingency M anager. Our review focused on the first five applications as they all directly relate to enterprise risk.

There is a lot of prepopulated content, and the tool makes it extremely easy to use and customize, taking very complex regulatory requirements and allowing one to quickly drill into a specific aspect and page to see specific items. There is a full history of reporting and auditing trails logged for all changes to policies and controls. There is also built-in awareness/training acceptance logging that allows one to track requirements for notifications to a user base. By clicking on a link embedded in the email with the update, a user acknowledges reading a policy or receiving updated notifications. The assessment engine is intuitive. One can build questionnaires by linking controls to policies. The questionnaire will present only relevant questions to the user, adapted on-the-fly based on the answers provided. The Threat and Vulnerability M anager provides the IT risk side of the equation. This application provides substantial correlation capabilities, it is easy to build imports from all the common scanners, it provides a powerful false-positive tuning tool, and it can run real time or batched. The asset management capability is complete enough to be a standalone offering or one can import assets from an existing tool or spreadsheet.

The reporting and dashboarding is done well with role-based integration to provide levels of access from admin to vendor. It tracks all aspects of the product and assessment lifecycle. There is a pleasing “what-if” analysis feature that allows users to detail out which requirements one would not comply with and even allows users to go into the exception workflow to ask for an exception.

The documentation that came with the product is all built in and is easy to use when needed. Support is included in the annual subscription price and provides technical support and product updates. When used as a complete set of applications, this solution delivers a lot of capabilities and makes the complex task of identifying, correlating, managing and remediating enterprise risk much easier.
McAfee Total Protection (ToPS) for Compliance v7.X

McAfee Total Protection for Compliance uses agent-based and agentless technology to audit, assess and report across managed and unmanaged systems, reducing the time and effort required for impact assessment of new threats and patching and compliance audits of IT systems. The tool combines McAfee’s Vulnerability Manager, Risk Advisor and Policy Auditor offerings and integrates them with its ePO tool to create a single platform for risk analysis and compliance reporting.

ToPS for Compliance is delivered as standalone software or via an appliance-based offering. It also can be installed on physical or virtual machines. It requires Microsoft Windows 2003 or 2008 and Microsoft SQL (standard or Express) 2005 or 2008. Typical deployments were reported to be a few days. We would expect to add in further time to customize reports, build the initial audits and tune the product for specific use.

ToPS addresses risk at the IT risk level. This product assumes compliance is a by-product of good security and focuses on assessing one’s IT, network and endpoint risk posture. The agentless option for gathering data from endpoints is a strong feature, allowing one to gather valuable information from systems with a zero footprint on those devices. The agent-based and agentless collectors can co-exist in the same environment so one has numerous deployment options.

ToPS proactively correlates threats with system-state information, including vulnerability data (cloud-based scanning only), patch level, configuration information, application data and countermeasure information to find critical assets at risk and optimize remediation efforts. ToPS is integrated with McAfee products and several third-party products to deliver closed-loop remediation. While last year we saw a very McAfee-centric offering, we did see more support this year for non-McAfee products and were told that the intent was to continue enhancing support for further third-party integrations.

The content library was complete and contained supported standards, like XCCDF and OVAL. The correlation was efficient, taking a single policy and applying it to all asset types and compliance requirements. The audit dashboard is an effective tool for viewing IT risk at a high level with the ability to drill down into detailed data. There is a built-in exception capability workflow allowing users to create “waivers” and manage the automated approval process. The risk management what-if analysis option gives one a solid tool for justifying IT spending. Too, one can model changes and show the risk impact to the environment. The reporting tools are powerful, allowing users to create, roll up and automate items and even use several reports to create a single report for the auditors. The correlation of threat, vulnerability and countermeasure data provides users with a very powerful prioritization capability for premier risks.

Support pricing was not provided, but we were told that 24/7 support is available for a fee based on size. Documentation was not supplied, so we cannot comment on that portion either. ToPS allows users to get the real measure of one’s security and risk compliance.

MetricStream Risk Management Solution v6.0

MetricStream Risk Management Solution enables organizations to identify, assess, quantify, monitor and manage their enterprise, operational and IT risks through an assessment-driven offering. MetricStream provides an integrated and flexible framework for documenting and assessing risks, defining controls, managing assessments and audits, identifying issues and implementing recommendations and remediation plans. The tool is part of the full MetricStream GRC offering. We reviewed the policy management and risk management components.

The tool is available as an on-premise software or as a hosted solution. There is support for moving from a hosted solution to an in-house platform. MetricStream Solutions are deployed as an N-tier web-based application architecture and built on standards, such as J2EE and XML. The application layer runs on Oracle. The user interface is web-based and done well. It delivers a large amount of information in an easy-to-navigate, non-cluttered and well-organized format.

There are built-in productivity and collaboration tools and a piecing geo-mapping tool for visualizing one’s enterprise. There are plenty of templates available for policies, risk, controls and issue management all built around the CO20 and ISO 30000 framework. One can create links among regulations, policies, risks, controls and organizations. This process takes complex relationships and makes correlating simple. A another solid outcome of this is an interconnection map that delivers a great graphical representation of all the above.

The tool is assessment-driven. Once created, the assessments are assigned via email to chosen parties. There are embedded links that will take them to their respective parts in the questionnaire. One answers specific questions and uploads any evidence required. Uploaded files are tracked to the individual question and available for any of the controls it supports. The modules are fully integrated. The risk and control assessments integrate with the loss management engine. One can keep an up-to-date profile using continuous risk assessments for vulnerabilities, threats and external data feeds, and tie it all together using key performance and risk indicators.

There is an integrated issue-management module that tracks actions and remediations. We could not tell from the documentation if there was an integrated ticketing system for assigning work, but the product does have great integration capabilities to other third-party solutions.

The Policy Management Solution provides a flexible framework to streamline the creation and management of corporate policies to facilitate accountability and foster communication. The solution enables companies to adopt an electronic and automated approach to the development, maintenance and communication of policies and procedures across the enterprise.

The annual support and maintenance cost is 20 percent for eight-hours-a-day/five-days-a-week, 25 percent for 24/5 and 35 percent for 24/7. By automating the entire risk management process through collaborative workflows and a common data model, the solution provides timely, actionable information.
Modulo Risk Manager v7.6

Modulo Risk Manager is a single, fully integrated platform for organizations to automate and unify their IT governance, risk and compliance (GRC) processes. Modulo Risk Manager automates the process of identifying, analyzing, evaluating and treating risks across the enterprise - reducing complexity and costs and offering visibility into the risk management process by identifying risk, measuring the impact to the business and tracking what the organization is doing about it.

Modulo Risk Manager is offered both as a hosted Saas solution or as an on-premise software deployment. The on-premise offering has two licensing models, perpetual (one buys it) or subscription (user’s hardware, rent the licenses). The on-premise solution requires M5 Server 2008 R2 64 Bit, .NET Framework 3.5 and M S SQL Server R2 Standard Edition 64 Bit. The web server has similar Win server requirements.

The product is a set of modules that includes risk management, policy management, telecommunications monitoring and supporting ongoing monitoring of risks and controls across the portfolio of client products, including vulnerability assessment, security information and event management, intrusion detection system and intrusion prevention systems products; vendor risk management; audit management; incident management; asset management and knowledge management. IT risk and vulnerability management integration is included and supports integration with popular vulnerability scanners.

Based on the ISO 31000 standard, the Risk Manager Modulo provides tools to inventory, analyze, evaluate and manage/mitigate risks. It delivers quantitative and qualitative information on identified risks and helps to prioritize actions. Risk is calculated using three dimensions: probability, relevance and severity. There is a complete incident management tool for addressing risks and non-compliant assets, allowing one to monitor progress through a comprehensive incident and workflow-management system. This function has been updated in this revision and provides better automated remediation options. One can easily automate the asset management process by providing asset inventory (both technology and non-technology-oriented assets, such as people, processes and facilities) that are imported from a number of third-party sources. The audit function is easy to use and, as mentioned above, has a ton of prepopulated content. The assessment process is done via email, but there is also a mobile application that allows users to not only answer questions but also upload evidence from a mobile device. The output of these modules provides a clear, comprehensive and prioritized view of risks and vulnerabilities, while integrating IT assets, resources, environment and processes into a single platform.

The reporting and visual dashboarding capabilities are as strong as any we’ve seen. One has role-based dashboarding, easy-to-use report editors and, most importantly, a correlated view of all risk aspects in the enterprise. Maintenance and support are free for the first year and cost 20 percent of the purchase price thereafter for perpetual licenses included in the Saas fees. This is a complete offering for managing risk. We wish we had more space to fully cover the other features we liked.

RedSeal Networks RedSeal v5.0

RedSeal v5.0 provides the intelligence necessary to proactively improve defenses, maintain continuous compliance and mitigate real-world risks by identifying all the available pathways of access and exposed vulnerabilities present across a network. The platform is focused on delivering continuous monitoring, compliance automation and risk measurement and control.

This product was the only solution delivered as an appliance. It is built on a Dell server platform and is customizable. The RedSeal 4200 is architected to offer a fast and efficient means of implementing RedSeal security software, and is designed to provide the most secure, scalable and dependable deployment possible.

This solution is more security than assessment-driven. A continuous monitoring offering focused on correlating IT, network and vulnerability data feeds, RedSeal identifies risk associated with one’s security effectiveness, as opposed to more policy- and compliance-driven tools.

There is a large library of supported vendor products allowing one to quickly and easily import network, security and vulnerability information into the tool. Once a user connects a device, RedSeal automatically builds out network maps and begins correlating this information with the configuration and vulnerability data and builds this into a threat reference library.

RedSeal is positioned to find and help eliminate gaps in one's security controls and, more importantly, prioritize or measure the impact of those gaps so that users can balance security investments with the highest return on those investments. RedSeal also takes into account the underlying business value of individual systems and assets, based on their importance to operations or retention of sensitive data, allowing users to prioritize mitigation even more effectively.

The network mapping function is a wonderful visual representation of assets and the interconnections that may exist on network and various controls in the environment. It helps to conduct a reachability study based on a threat and to determine where and how far that threat could propagate in an enterprise, which is a valuable analysis tool. This provides a great opportunity to mitigate either a threat or a vulnerability before the actual compromise or exploit. The correlation capability of the RedSeal product takes a loss of the noise out of the traditional vulnerability scan process by providing a real risk priority based on the entire environment.

RedSeal is not an assessment or audit tool, but it does correlate risk to various controls for compliance regulations, like PCI, NIST and FISMA, creating reports that show gaps in deployed configurations/controllers. For example, for PCI, it may ask: Is my credit card data isolated properly? One also can model what the network should be doing to be in compliance.

We liked the attack simulation feature, which gives one the ability to model a threat based on the known access and vulnerability information and determine, step by step, what could be breached. There is a dashboard component that provides some high-level management-level details so that one has a snapshot of the key risk posture items. Further, there is built-in reporting capabilities that provide the data roll-up from most of what we described above.
### RSA Archer eGRC Suite, RSA Archer eGRC Platform v5.1.4

RSA Archer Risk Management enables users to proactively address risks to reputation, finances, operations and IT infrastructure as part of a governance, risk management and compliance (GRC) program. The software provides a central GRC management system for identifying risks, evaluating their likelihood of impact and then tying those to mitigating controls and tracks resolution progress.

Risk Manager is part of an Enterprise GRC product portfolio sold and licensed as modules. These modules include: audit, policy, risk, compliance, enterprise, incident, vendor, threat and business continuity management. This product is offered as either on-premise software or as a hosted, rapid-deployment model. The platform is composed of three logical tiers including interface, application and database tiers. The platform itself is deployed on two physical tiers that can be hosted on one physical or deployed across multiple servers. The platform uses a common data model across all of its solutions and applications. The user interface is common for all modules and tabs are simply activated via licensing.

The risk module can be used standalone, but, in reality, users will want to employ it in conjunction with the enterprise (asset tool), incident and threat management modules for a complete view of risk. RSA Archer Platform can integrate with hundreds of different solutions, as long as the offering can be an extreme technical difficulty. This product is offered as either on-premise software or as a hosted, rapid-deployment model. The platform is delivered as either on-premise software or as a cloud-based offering. The on-premise solution deploys in a two-tier web server/database server model, requires MS Windows 2008 Server, SQL 5.0 or higher, .NET Framework and proper MS SQL licensing.

### Rsam eGRC Platform v7.5

The Rsam Enterprise GRC platform is a fully integrated, modularized platform supporting full GRC or individual module deployments. The components include: assessment, compliance, issues and remediation, threat and vulnerability, audit management, incident management, policy and exception management, controls testing, vendor risk, and enterprise risk/risk register. The platform is delivered as either on-premise software or as a cloud-based offering. The on-premise solution deploys in a two-tier web server/database server model, requires MS Windows 2008 Server, SQL 5.0 or higher, .NET Framework and proper MS SQL licensing.

### OVERALL RATING

<table>
<thead>
<tr>
<th>Value for money</th>
<th>Ease of use</th>
<th>Performance</th>
<th>Documentation</th>
<th>Support</th>
<th>Ease of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>★★★★</td>
<td>★★★★</td>
<td>★★★★★★</td>
<td>★★★★★</td>
<td>★★★★</td>
<td>★★★★★★</td>
</tr>
</tbody>
</table>

### Strengths
- Robust gap/risk reporting and impact analysis
- Maturity shows in the user interface

### Weaknesses
- Not really a weakness

### Verdict
- This is an enterprise business and IT risk solution that is very well put together. Users will like a lot of the “little things” that have gone into the product.

### Contact
- emc.com

---

### Details
- **Vendor**: RSA
- **Price**: A mid-range configuration starts at approximately $55,000 and can vary depending on what is being managed and the scope of the deployment.
- **Website**: www.scmagazine.com
Skybox Security Skybox View
Enterprise Suite v6.0

The Skybox View Enterprise Suite is a set of tools for firewall management, network compliance assessment, and risk and vulnerability management. It is built on a common platform for data collection, network modeling, attack simulation and reporting. Skybox produces a comprehensive model based on network topology, assets, vulnerabilities and threats, and assists in identifying critical security concerns in large networks. Skybox solutions conduct risk and threat assessments and use attack simulation to identify risky access paths and exploitable vulnerabilities.

The product is sold as a software offering with deployment options. All components of the software can be loaded on a single server-class platform of the customer’s choosing, on the Skybox 5000 appliance or on a virtual appliance. Operating systems supported for the customer-supplied server include Windows, CentOS 5 or Red Hat Linux.

The Risk Control portion automatically correlates vulnerability scan data with information about network topology, device settings, asset values and known threats. Risk Control uses attack simulation to find vulnerabilities and access paths that can be exploited. One can identify, prioritize and eliminate critical risks and vulnerabilities. There is an updated summary page in this version that is configurable, role-based and gives more granular levels of rule definitions. The main focus of this tuning is to deliver a highly prioritized view of risk so that users can most effectively deploy resources. There is a pleasing multitiered tool that provides options for suggested fixes. As well, there is an integrated workflow and ticketing tool for automating tasks. Assets can be imported from other asset management or GRC tools, though there is some work involved in initially setting up and classifying assets.

Skybox generally works with more than 38 vendors and devices, supporting firewalls, routers, switches and intrusion prevention systems. Skybox also provides a web-services API (IXML) to allow quick integration to unique or legacy devices. This integration allows users to easily gather layers 2 and 3 network information or if needed. Skybox natively works with more than 38 vendors and devices, supporting firewalls, routers, switches and intrusion prevention systems. Skybox also provides a web-services API (IXML) to allow quick integration to unique or legacy devices. This integration allows users to easily gather layers 2 and 3 network information or any flat file format. We also would like to note that data gathering can be done using both agentless and agent-based clients. This feature gives a lot of flexibility in gathering information from devices.

There is a built-in change-management workflow tool and also a threat management workflow tool. Users can set up their own threats in the dictionary without having to import information from a scanner. Reporting was good and included the ability to track to key performance indicators in a clean dashboard presentation. The reporting roll-up was powerful, sorting and filtering by vulnerability type, vendor and more. Users also have a tool to perform what-if analysis and modeling configuration changes prior to putting them into production. Users have a live, a what-if and a forensic work space to perform investigations based on past or other models.

There are two levels of support available: eight-hours-a-day/five-days-a-week and 24/7. The premium option has additional features, such as an assigned technical person with direct dial access. The pricing is 18 percent and 22 percent of net license and hardware price.

Symantec Control Compliance Suite v11

The Control Compliance Suite enables enterprise IT security organizations to define security and compliance-related policies. These are mapped to detailed technical checks and/or specific procedural questionnaires that measure overall risk and compliance within the IT environment.

The product is delivered as an on-premise software offering. Besides the hardware platform, the requirements include MS Windows Server 2003 SP2 or 2008 and Microsoft SQL Server 2005 SP2.

The Risk Manager component is designed to provide a quick view into IT risk. The process sets out to define an asset, either physical or business assets. The next step is to help visualize and document IT risk for the particular asset. Based on the importance of the particular line of business, assets and more, a “risk threshold” can be set to alert owners when the security of those assets is in jeopardy. The tool will help prioritize remediation tasks based on risk, not severity. The user interface is well laid out and easy to use, and navigation is Microsoft-like. Policy setup is done through templates or users can import their own. The product comes with more than 150 mandates, best practices, regulations and more, that are predefined and ready for use. Using the same tool, users map controls to policies. The policy portion is integrated with the risk module and remediation actions can be initiated with granular instructions to rectify non-compliance and mitigate risk.

Once policies and controls are done and mapped, users can assess the environment. Assessments can mean many things: one can assess against standards, use the vulnerability manager to discover critical vulnerabilities, evaluate procedural controls or integrate data from various third-party sources to review. Security-related information can be collected using a general-purpose external data interface that enables the enterprise to broaden the risk and compliance view by leveraging other security products they have in their environment. Imports are supported via Open Database Connectivity (ODBC), web API, or any flat file format. We also would like to note that data gathering can be done using both agentless and agent-based clients. This feature gives a lot of flexibility in gathering information from devices.

There is an integrated workflow tool for scheduling and assigning tasks or one can integrate directly with third-party ticketing systems. Reporting, charting and dashboarding were all well done. A dynamic dashboard capability pulls everything together by presenting a customized view of risk and compliance for specific areas. Dashboards can be defined to address specific needs and include drill-down capabilities to yield specific, detailed information as needed.

Support is available at 25 or 29 percent of the cost of the software. Basic maintenance and essential support includes a comprehensive menu of telephone, online and tracking services. The documentation was complete and easy to follow.
**GROUP TEST | Risk & policy management**

### AlgoSec Security Management Suite

The Security M management Suite from AlgoSec provides many features for both firewall policy and risk management. The suite can come bundled in a single appliance, and includes two key components, the Firewall Analyzer and FireFlow. The Firewall Analyzer is the larger of the two components. Administrators can use it to perform auditing, compliance and risk analysis along with optimization and change monitoring. FireFlow allows administrators to manage firewall policy change through automation and workflows to ensure that submitted changes are compliant with regulatory standards.

We found this appliance to be quite easy to set up and manage. All administration is done via a lucidly designed management interface, which we found to be comfortable to navigate and easy to use. We also found this appliance to offer a lot in the way of configurability and automation. From the interface, we found it easy to interact with firewalls and devices, such as routers and switches. This appliance also comes loaded with many out-of-the-box workflows ready to go for the Fireflow component of the suite. Using these workflows, an administrator can easily double-check changes before they are made to the infrastructure, including risk and compliance assessments. If the change is not needed or unnecessary, and optimal design recommendations, FireFlow also can submit changes to select devices using its ActiveChange function, which helps eliminate human input errors. Firewall Analyzer breaks down to three major components: The first is risk analysis. The analyzer can compare security policies to a database of industry best practices and identify the associated rules. Once rules are identified this tool can then define various configurations to which devices must be compliant and report on their status. Furthermore, the appliance monitors for changes and can provide instant feedback if the change may create risk or take network sections offline. The second component is compliance standards. This offering can provide full compliance checks against many standards right out of the box. The final component is optimization. The FireFlow component of the suite can be a great value for the money. The AlgoSec Security Management Suite provides a number of features and functionality that make both policy change and risk management easy and seamless, while ensuring that compliance needs are met and adhered to.

### FireMon Security Manager with Policy Planner and Risk Analyzer

The FireMon Security Manager with Policy Planner and Risk Analyzer is the ultimate policy and risk management tool. The two major components of this product are the Security Manager, which includes the Policy Planner running on a single, purpose-built appliance, and the Risk Analyzer, which is software that must be installed on a client machine running Microsoft Windows 7 or Mac OS X. The two components work in tandem to provide full-scale policy and risk management and are loaded with features. The initial installation consists of setting up the appliance and then installing the Risk Analyzer software. The appliance setup process is done by connecting a monitor and keyboard to the appliance and running through a short setup wizard, which sets network and hostname configuration. At the completion of the setup wizard, the Risk Analyzer package can be easily installed on the client machine and the appliance can be added to the management console.

After spending some time with the appliance and management console, we found this product to offer some robust features and functions. On the policy management side, this tool offers full configuration management of firewalls, routers, switches and load balancers. Using Security Manager, administrators can run assessments of device configurations against industry best practices and compliance standards, and then the product will offer recommendations for policy cleanup and other options. This product also can run instant reports based on regulatory and compliance standards providing deep insight to ensure regulations are met and compliance is maintained. As for risk management, this product attacks risk on two fronts. First, the risk analysis engine determines possible attack paths into the network, as well as uses penetration test results to provide a full-scale score based on risk level. The second way this product can help manage risk is using the Policy Planner component. The Policy Planner offers a full, change management workflow that enables administrators to simulate proposed access changes to measure possible risk before the changes are implemented and rolled out.

Documentation included a getting-started PDF along with full user and administrator guides. The getting started guide provided a detailed overview of the installation process, as well as other useful information on basic configuration. The user and administrator guides focused on advanced configuration along with how to use the features and functions of the product. We found all documentation to be well-organized and easy to follow with many step-by-step instructions, screen shots and configuration examples. We found this product can be a bit expensive for some, but we also found it to be a reasonable value for the money. Customers can purchase the FireMon Security Manager Starter Kit, which includes perpetual licenses for one server appliance, two firewalls and associated management consoles, two switches/ routers and one year of support for all products, along with the appliance itself, for just under $12,000, adding on the Policy Planner and Risk Analyzer at an additional cost.

### DETAILS

**Vendor**

- **AlgoSec**

**Price**

- Starting at $10,000.

**Contact**

- algosec.com

**RATINGS**

- Ease of use: ★★★★★
- Performance: ★★★★★
- Documentation: ★★★★★
- Support: ★★★★★
- Value for money: ★★★★★

**OVERALL RATING**: ★★★★★

**Strengths**: Many features and functions, including several out-of-the-box templates for managing compliance and risk.

**Weaknesses**: None that we found.

**Verdict**: Very strong feature-rich product.

**Vendor**

- **FireMon**

**Price**

- Starts at $11,995; Policy Planner and Risk Analyzer are additional costs.

**Contact**

- firemon.com

**RATINGS**

- Ease of use: ★★★★★
- Performance: ★★★★★
- Documentation: ★★★★★
- Support: ★★★★★
- Value for money: ★★★★★

**OVERALL RATING**: ★★★★★

**Strengths**: Powerful and robust tool that offers a lot of risk and policy management functions.

**Weaknesses**: Can be cost prohibitive to some.

**Verdict**: Lots of power and full-featured, but can be a bit pricey.

---

*SC • June 2012 • www.scmagazine.com*
Lumension Risk Manager

Lumension Risk Manager is a piece of a larger suite called the Lumension Compliance and IT Risk Management platform. However, that does not mean that Risk Manager cannot do a lot without the other components of the suite. This product is a feature-rich risk management platform that can take results from vulnerability scans, as well as anti-virus scanners, and correlate the results into useful information as to the risk and security posture across the network. Administrators also can use Risk Manager and the risk intelligence engine to correlate internal policy against many compliance standards and regulations.

The review of this product was conducted using a virtual evaluation server, which already had the product installed and up and running for us, so there was not much to do in the way of installation and configuration. However, we do know that the product is a software-based solution and requires a dedicated server running Windows Server along with access to a Microsoft SQL Server database either running locally on the server or accessible on a separate server. The installation of the software engages all the necessary components, including the web-based management console. We found this to be fairly easy to navigate with an organized tab-top navigation structure. A major part of this product is not only managing risk but also maintaining compliance. Using this tool, administrators can easily report and evaluate on compliance of many devices across the network and make sure they are in line with compliance standards. Reports can be easily generated along with remediation modeling of possible scenarios to determine if certain remediation tasks will boost or hinder the security posture of the network. This product also contains many automated workflows which can help streamline the assessment process and provide targeted results quickly and easily.

Documentation included only a short evaluation guide. The evaluation guide did provide a solid overview of using the product for various scenarios and had many step-by-step instructions along with configuration examples and screen shots. We would have liked to see an administrator-guide link or some kind of access to product documentation, either in the interface itself or in the start-menu shortcut folder on the server itself.

Lumension offers an excellent amount of both no-cost and paid support. Customers can access many options as part of their subscription cost of the software. Some of these options include 8 a.m. to 5 p.m. phone-based technical support, along with email support with one-day response and access to an online portal and knowledge base. Paid support offers a lot more, including 24/7 phone-based technical support, accelerated response times, remote health checks, dedicated technicians and many other features.

With a price of just above $33,000 for a perpetual license, this product can be quite expensive for many environments. However, Lumension does offer a subscription-based model for those who wish to pay on an annual basis. We found this product to be an average value for the money. While it does offer some solid features, it is quite expensive given that the scope of the product is limited.

NetIQ Secure Configuration Manager

The Secure Configuration Manager from NetIQ offers a full systems and configuration management platform to manage both risk and policy across many network assets. Using this product, administrators can easily run system configurations against many compliance standards and obtain a report on systems that do not meet policy requirements. This product also allows for a risk-based approach to remediating systems based on criticality and severity of the misconfiguration.

We found installing this product to be not as straightforward as the documentation outlines. The first step in installing the software is to get a 64-bit Microsoft Windows Server up and running, which we found was one of the easiest parts of the deployment. After that, we had to install Microsoft SQL Server 2008 and that was not also a problem. Then it started to get tricky. This product uses the components from 11.6.0 to run the web-based management console, so there are quite a few steps to go through to enable Server 2008 to run the legacy version.

Our overall installation from this point forward was plagued with errors and troubleshooting. However, once we fixed all the problems and were able to get all the prerequisites installed, the rest of the installation went relatively smoothly.

The setup process of the software itself is guided by a set of setup wizards, which help make the installation of all the components and hot fixes quite seamless, but we would have liked to see a more streamlined process for installation of the product overall. Once everything was installed, we found this product to be quite easy to use. The management console was comfortable to navigate and we found configuration of the product to be simple and straightforward. Once inside the management console, we found this product to offer a lot in the way of features and functions. There are many dashboards and visual aids that help aid in a bird’s-eye view of the systems and security posture of the network overall.

Documentation included many PDF manuals and documents. Some of these included installation guides for all the various components of the product along with a full user guide for in-depth information on configuration and use of product features. We found all documentation to be easy to read and to include many screen shots, configuration examples and step-by-step instructions.

NetIQ offers customers no-cost 12/5 phone and email technical assistance, as well as access to an online support area. This includes many resources, including a knowledge base, user forums and useful documentation and downloads. Customers also can purchase additional support in premium and platinum levels as part of a contract. These levels include access to advanced aid, such as 24/7 technical assistance and other options.

At a price starting at around $1,200 per server license for the software, we find this product to be an excellent value for the money. The Secure Configuration Manager offers a great amount of risk-based policy management that can ensure that critical systems are compliant with both security and regulatory policies.
GROUP TEST | Risk & policy management

NetWrix Change Reporter Suite

The Change Reporter Suite from NetWrix offers full change management across an entire network infrastructure. Chances are that if something has been changed, this product will know about it and be able to report the alterations to those that need to know. This appliance can monitor for changes almost anywhere on the network, including Active Directory, file servers, Microsoft Exchange, storage appliances (such as NetApp or EMC), virtual and physical infrastructure, and SQL Server databases, among many others. Using this suite, administrators can easily keep an eye on the environment and know who changed what, what the value was changed from and to, and, more importantly, when and where the change originated.

We found installation to be simple and straightforward. However, it can be a tad tedious. The suite includes many installers that must be implemented for the tool to operate. The first step in installation is to deploy a Microsoft SQL Server or have one available to house the backend database. After the SQL server is up and running, the various components must be installed. From there, all administration is done via a management console that has the look and feel of a Microsoft management console, so most administrators will feel right at home navigating and managing the product.

We also found that setting up the environment to report changes was easy. Once set up, we were getting results almost instantly. One thing we really liked about this product was the large amount of directories and other places it could plug in to, as well as how easy it was to configure change management across many types of devices. The final component to the Change Reporter Suite is compliance management. The suite comes pretty much ready to go to aid in managing compliance standards throughout the environment and making sure a change will not affect policy compliance. Using the built-in Auditurance technology, Change Reporter Suite can provide detailed reports that include information on every change that has occurred throughout the enterprise. Documentation included many guides and manuals for deploying and managing the various components of the product. We found all these guides to be helpful and well-organized with many screen shots and easy-to-follow instructions, but we would have liked to see a more streamlined documentation structure. Consolidating the many documents into a full administrator guide would not only be more efficient, but also ensure that parts of the documentation will not get lost or deleted accidentally.

NetWrix offers no-cost and paid support options to customers. Customers can access many online aid resources at no cost, including full, unlimited access to a user support forum and 20-day access to a knowledge base and trouble ticket submission portal. After the first 20 days, customers can obtain a contract, which includes unlimited access to the knowledge base, as well as full email- and phone-based technical support.

With a price starting at just over $18 per user for up to 150 users, we find this product to be a good value for the money. The Change Reporter Suite offers a lot of integration options to help monitor and manage changes throughout the enterprise.

New Net Technologies NNT Change Tracker Enterprise

NNT Change Tracker Enterprise from New Net Technologies offers a full suite of change management, file integrity, monitoring and policy management tools for network devices, including firewalls and systems, throughout the network environment. Administrators can use this tool not only manage changes to devices, but also audit the network for vulnerabilities and policy compliance. Administrators also can see deep into changes made across the environment, including who made the change and when, even if the change happened between scheduled reports. This provides a great benefit over simply comparing the data between the reports as changes can be missed or overlooked.

We found setup and deployment of this product to be quite straightforward. The initial setup is done by running a set of executables to install all the various components. After installation is complete, all management is done via a management console, which we found to be easy and comfortable to navigate through. The management console features an easy-to-follow tab-top navigation structure that is well-organized and we had no trouble becoming accustomed to browsing around and configuring the product. Another nice feature that added to the experience was the ability to scan the network and automatically add devices from the scan directly, making the initial setup piece almost effortless.

Change Tracker Enterprise also comes loaded with many standard compliance templates for regulatory requirements, including PCI DSS and ISO27000, among others. However, administrators also can make custom templates that meet specific needs of the environment or organization. Overall, this product has some very useful features and functions packed into an easy-to-use application.

Documentation with the tool included full administrator guides for both Windows- and Linux-based installations. We found both to be easy to follow and to include many screen shots, step-by-step instructions and configuration examples. We also found the guides to include an excellent amount of detail and in-depth explanations on how to install, configure and use the product’s features and functions.

New Net Technologies offers general help to customers at no cost, but to get full support customers must purchase a contract. Support options available as paid include both eight-hours-a-day/five-days-a-week and 24/7 levels, which give customers access to both phone- and email-based technical assistance. A limited no-cost support options.

Verdict Although the application is quite focused, this one has everything it needs at an excellent price.
SolarWinds Network Configuration Manager

The SolarWinds Network Configuration Manager offers the ability to check all network devices, including routers, switches and firewalls, throughout the network environment against compliance and policy templates. This product includes a vast amount of vendor flexibility and can manage devices from Cisco and Juniper, as well as many other devices, such as Nortel and 3Com. This flexibility guarantees that pretty much any device anywhere in the network can be managed using this tool. Furthermore, this product can generate multiple types of reports that can be launched on demand or scheduled and delivered via email to those that need to see them.

Overall, we had a good experience with this product in the way of ease of use. The installation was quite simple and took only a few minutes after launching the downloadable installer. The installer executable put in place all the necessary components to run the product and once complete all management and configuration is done via the management console. We found the management console itself to be relatively simple to use, but it did take us some time of browsing around to become thoroughly comfortable with the interface. The main dashboard is the first thing that pops up on the screen after logging into the console. We found this to provide a lot of great information, including active alerts at a glance along with an overview of all of the devices in the network.

A few of the dashboard, the rest of the interface is based around configuration management, and there is a lot of functionality in this area of the application. It is here that administrators can easily view a configuration summary, manage configuration and policy templates, view a full network inventory list and manage compliance. We also found this product to offer quite a few preloaded compliance policy reports. Adding to the overall compliance piece is the ability of this product to interface directly with user-created policy templates that are shared on the SolarWinds online community thwack.

Documentation included quick-start and full administrator guides. The quick-start guide offered a great amount of detail on how to install the product and get a base configuration in place, while the administrator guide focused on advanced configuration and use of the product features. We found both to be well-organized and to include many step-by-step instructions that were easy to follow, but there was a lack of screen shots throughout the documentation. We really like to see screen shots because they help more clearly illustrate how to configure the product and where on the interface to click rather than having the user scan around the interface trying to find a radio button or link. SolarWinds offers the first year of product support as part of the initial purchase price of the product. After the first year, customers can purchase additional assistance starting at around $500 per year based on support-tier level.

At a price just shy of $2,500, including the first year of support, we find this to be a very good value for the money. This product brings together a strong combination of policy management and compliance features that can make managing network devices more convenient for administrators.

Tripwire Enterprise

Tripwire Enterprise brings together policy management, change management and file integrity monitoring under one easy-to-manage platform. With Tripwire Enterprise, administrators can use a combination of an agent-based and an agentless deployment to collect, assess and report on server, database, endpoint and network device configurations throughout the entire enterprise environment. This tool is also leveraged by a couple of key components, which include Asset View and Fast Track. More explanation on those in a minute. First, we take a look at deployment and installation.

This product is software-based, so it must be installed on a server in the environment. Installation of the product itself is easy and is done by simply running an executable, which launches a cleanly organized setup wizard. At the completion of the wizard, the product installs all the necessary components, including the management console. A first installation is complete, all management is done via the web-based management console, which we found to be well-organized and easy to navigate with a clean look and tab-top navigation structure. The other thing to note about the management console is the clean dashboard views. The dashboard is one of the first things that an administrator sees when they log into the console and it is loaded with a plethora of useful information, including authorized versus unauthorized changes, changes by application, and many other charts and graphs. This gives the administrator an instant view of what’s happening and if anything needs immediate attention.

Tripwire Enterprise also lets you leverage a library of more than 25 unique policy sources that cover a large amount of policy and platform combinations. These policies include not only regulatory compliance guidelines, such as PCI, HIPAA and NERC, but also hardening guidelines for software vendors, security policies and country-specific standards and best practices. This massive library allows administrators to find and deploy all policies that apply to their environment or organization.

Documentation included installation, user and reference guides. We found each to contain a good amount of detail and easy-to-follow, step-by-step instructions, along with quite a few screen shots and configuration examples. Tripwire offers only paid support to customers, who can choose from standard and premium levels at a starting cost of $199 and $459 per year, respectively. Standard support includes 12/5 phone- and email-based support, as well as access to a web-based support portal, which includes resources such as a knowledge base, resource library, support forum and product downloads and documentation. Premium support includes the same portal access and also adds full 24/7 phone- and email-based support.

Pricing for Tripwire Enterprise is a little tricky, but customers can choose from a wide variety of pricing options. The Express Console version, designed for smaller environments, starts at just under $700, but there is also an Unlim- ited Console available for $7,000. Those prices license the console as well as endpoints. However, file system monitoring and network device monitoring is an extra cost. We find this product to be a very good value for the money overall.
Tufin Security Suite

Back again this year is one of last year’s favorites. The Tufin Security Suite is back with some of the same solid features that made it an excellent product last year, but it also has some new features that again continue to separate it from the pack. Tufin Security Suite is made up of two major components. The first is SecureTrack, which can scan and access firewalls, routers and switches to make sure they meet compliance and security policy. The second is SecureChange, which automates policy change across the enterprise network environment.

We found this product to be easy to both set up and configure. The initial setup process consists of connecting the appliance to the network and, using a web browser, navigating to the default address assigned to the appliance. Once there, we were prompted to run a short setup wizard, which not only assists in setting up the basic network information, such as IP address, but also allows for license input and other basic configurations to get the appliance up and running. After the wizard is complete, all further administration and management is done using the web-based management console. Overall, we found this console to be easy to navigate with an intuitive look and feel, and we instantly felt comfortable moving around and configuring the appliance for the environment. Something new this year was the addition of a dashboard to the console, which provides a nice overview with a good amount of useful at-a-glance information.

Now on to functionality. As said earlier, there are two components of the suite that work in tandem to make this product a comprehensive policy and risk management tool. SecureTrack offers administrators the ability to interface directly with routers, switches and firewalls throughout the network and manage changes to rules and policy optimization and run built-in compliance reports against the infrastructure for auditing purposes. SecureChange comes in to add to the overall flexibility and comprehensiveness of the suite. Using SecureChange, administrators can run changes through a customizable workflow to ensure a change is not unnecessary, could cause vulnerabilities in the infrastructure or is out of regulatory compliance. After the change has passed through the workflow and is proven to be acceptable, it can be automatically pushed out to certain devices through an automated provisioning process.

Documentation consisted of the usual wares of a short quick-start and a full operations guide. The quick-start guide offers a detailed explanation of the initial setup process, including full screen shots and step-by-step instructions for going through the setup wizard. We found all documentation to be well-organized and easy to follow.

Tufin offers no-cost email- and phone-based technical support to customers during business hours. Customers also can purchase additional aid through professional services for on-site installation at an extra cost.

At a cost of $25,000, we find this product to be an excellent value for the money. The Tufin Security Suite offers a comprehensive set of features and functionality that cross paths of both policy and risk management.

Viewfinity Privilege Management

Any security administrator knows that they are only as strong as their weakest link. We have seen a lot of products in this group that focus on making sure devices are in compliance with the security policy, but what about the users? Users with too many privileges or permissions are just as dangerous as a non-compliant machine or network device. This is where Viewfinity fits into the group. Using Viewfinity Privilege Management, administrators can control privileges for users throughout the environment and escalate privileges as needed on a case-by-case basis or as part of an overall policy.

Setup of this product requires Microsoft Windows Server 2008 running IIS and Microsoft SQL Server 2008. Once the server is set up, the installation of the Viewfinity server itself is quick — guided by an easy-to-follow setup wizard. The wizard aids in setting up general server components, as well as the necessary connections to the backend database and the web-based management console. At the completion of the wizard, all further configuration and management is done via the web-based management console, which we found to be well-organized with a clean look and feel. Navigating around the interface is comfortable and fluid, as well as intuitive.

Viewfinity Privilege Management offers a lot in the way of functionality and allows for many flexible and granular policies to be easily deployed throughout the enterprise. This product also features a fair amount of automation capabilities, including policy creation and management, using compliance-based or custom policies and full automated user analysis to determine the needs of specific users or groups of users. This product also plugs into Active Directory directly to help streamline user and group management through Microsoft Group Policy. Furthermore, this product offers full auditing of privileged accounts and account activity.

Documentation included server installation, quick-start and full operations guides. The server installation guide illustrated the full process for setting up the Viewfinity server along with detailed instructions on how to install all prerequisites to get the server up with an initial configuration. The quick-start guide took over from there illustrating some basic configuration steps and a brief overview of the product features and functions. The operations guide provided a more in-depth look at using advanced features and configurations. We found all document to be well-organized.

Viewfinity only offers customers paid support as part of their subscription costs or as part of an annual agreement. Customers with contracts can access either eight-hours-a-day/five-days-a-week or 24/7 phone- and email-based technical support, along with a full portal available online.

This product can either be quite cost-effective or very cost-prohibitive based on the size of the environment. Viewfinity Privilege Management is licensed on a per-node basis with prices ranging from $40 for a perpetual desktop or laptop license to $200 for a perpetual server license. Volume discounts are available, but in a large environment it could get expensive quickly. Overall, we find this product to be a good value for the money due to its comprehensive feature set and ease of management and automation abilities.

---

**GROUP TEST | Risk & policy management**

**Tufin Security Suite**

**Vendor:** Tufin Technologies

**Price:** $25,000

**Vendor Details**

**Ease of use:** ★★★★★

**Performance:** ★★★★★

**Documentation:** ★★★★★

**Support:** ★★★★★

**Value for money:** ★★★★★

**OVERALL RATING:** ★★★★★

**Strengths:** Full-featured policy and risk management tool.

**Weaknesses:** None that we found.

**Verdict:** Very strong offering with all the bells and whistles that is a must-have.

---

**Viewfinity Privilege Management**

**Vendor:** Viewfinity

**Price:** Licensed on a per-node basis with prices ranging from as low as $20 up to $200 per device.

**Vendor Details**

**Ease of use:** ★★★★★

**Performance:** ★★★★★

**Documentation:** ★★★★★

**Support:** ★★★★★

**Value for money:** ★★★★★

**OVERALL RATING:** ★★★★★

**Strengths:** Automated account privilege management with easy-to-deploy policy.

**Weaknesses:** Can become expensive for large environments.

**Verdict:** Well worth attention for its solid feature set, ease of deployment and use and performance. Narrow application, but what it does, it does very well.

---

48 SC • June 2012 • www.scmagazine.com
Big Data requires new skills

Today’s firms must identify people who have knowledge from disparate areas, says Tracey Wilen-Daugenti.

The computational world of the 21st century will require a particular new skill set from workers - and innovators, business recruiters and IT professionals would do well to take notice. A study by the Apollo Research Institute identified the ability to translate vast amounts of data into abstract concepts and to understand data-based reasoning. Workers will increase their value by acquiring more sophisticated abilities in statistical analysis, quantitative reasoning and expertise in using modeling and simulations. At the same time, they will need to temper this “wonkiness” with a clear understanding that models can simulate reality, but don’t recreate it. The ability to act in the absence of data is also important.

Apollo identified the concept “transdisciplinarity” to define a need for literacy in and the ability to understand concepts across multiple fields of study. Because the complexity of modern world problems calls for input from more than one discipline, transdisciplinarity will transcend the specialization of the 20th century. The ideal worker has been described as “T-shaped,” that is, having depth in at least one specialization, but also a breadth of understanding across a range of specialties. To help teams strike innovative sparks, firms will need to do more than simply bring people of various disciplines together. They must identify people who have real-world skills and knowledge from seemingly disparate areas.

“Design mindset” is the ability to represent and develop tasks and work processes for desired outcomes. This skill set has clear implications for workplace design. A neurobiologist Fred Gage argued, “Change the environment, change the brain, change the behavior.” Workstations, room design and corporate campuses can be designed to enhance workers’ cognition and creativity.

Massive data collection has the potential to increase security, but...
World’s No. 1
Antivirus and Internet Security

Special offer: Buy 1 license, get 1 free!
For a limited time only, purchase award-winning ESET NOD32® or Smart Security Business Edition products and receive an equal number of complimentary Exchange seats.
Promo code: 2012Q2PROMO
Valid 4/3/2012-6/30/2012. For terms, visit http://go.eset.com/us/q2promo-trial

Why choose ESET for malware protection?
• Fast scanning speed
• Light resource utilization
• Ease of manageability
• Proprietary ThreatSense® for detection of unknown threats

Virus Bulletin Awards  Success ratio (%)

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

Selected Antivirus Vendors (not a complete list)

©1999-2012 ESET. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET. All other names and brands are registered trademarks of their respective companies.