FEATURES:

SHARING THE PIE

Georgia Tech researcher Christopher Smoak helped create an intelligence system for threat information collaboration P18

A fine balance
Polish-born Canadian Rafal Rohozinski parleys his nonprofit initiatives exploring the internet’s shadier regions into a for-profit business PC1

Embracing BYOD
Even the government acknowledges that it can’t prevent the use of personal devices P26

Measuring success
Gauging performance does not necessarily result in enhanced security, but quantifying risk is still vital P28
REGULARS
4 Editorial Staying out of the headlines
8 Threat report Russian authorities apprehended the person believed to be behind a banking-trojan botnet
10 Threat stats 6.5 million LinkedIn passwords were posted online
12 Update The Canadian government attempted to bar foreign IT companies from bidding on the construction of its new telecommunications system.
13 Debate The easiness of Flame may have been what thwarted traditional anti-virus technology
14 Two minutes on... U.S. cyber coordinator moves on
15 Skills in demand IT business continuity and disaster recovery specialists are needed
16 From the CISO's desk First: Define critical infrastructure, by Mark Clancy, managing director and CISO for The Depository Trust & Clearing Corp.
17 Opinion Infrastructure wake-up call, by Chris Petersen, co-founder and CTO of LogRhythm
18 Sharing the pie Georgia Tech researcher Christopher Smoak helped create an intelligence system for threat information collaboration.
26 Embracing BYOD Even the government acknowledges that it can’t prevent the use of personal devices for work-related functions.
28 Measuring success Gauging performance does not necessarily result in enhanced security, but quantifying risk is still vital.
31 Product section Call them pervasive, ubiquitous or widespread, the fact is that today’s threats are everywhere and of just about every type one can imagine.
32 Group Test: Endpoint security In today's more evolved enterprises, all of the endpoints are managed and coordinated through a single junction. However, there are some surprises in the marketplace.
38 Last word New partnerships required, by Raymond Choo, senior lecturer at the University of South Australia.

FEATURES
18 Sharing the pie Georgia Tech researcher Christopher Smoak helped create an intelligence system for threat information collaboration.
26 Embracing BYOD Even the government acknowledges that it can’t prevent the use of personal devices for work-related functions.
28 Measuring success Gauging performance does not necessarily result in enhanced security, but quantifying risk is still vital.

FROST & SULLIVAN
“Frost & Sullivan recommends that customers invest in annual ethical hacking assessments by leading companies such as High-Tech Bridge.”
Frost & Sullivan’s Whitepaper, April 19th, 2012

HIGH-TECH BRIDGE SA
SWITZERLAND - GENEVA - WORLD TRADE CENTER II
Staying out of the headlines

After talking to her office-working brother, my hairdresser the other day was extolling the benefits of using numbers, capital letters and other characters to create the various passwords she enlists to access countless private accounts daily. Up until that impromptu conversation during an Independence Day barbecue with family, she had never given usernames and passwords much thought. Most of the time, her private email address and dog’s name seemed to suffice.

Her brother hadn’t really paid much attention to his personal (or professional) passwords either. However, after some well-publicized breaches of credentials at the likes of LinkedIn, eHarmony and Formspring, his company felt the need to invest in some end-user security awareness and training.

Unbeknownst to his organization’s executives, their decision could not have been more timely given the now-bedeviling news that some 450,000 Yahoo members have seen their usernames and passwords stolen by the hacker group D33ds Company. Yahoo seemed to make the thieves’ job quite a bit easier by shockingly failing to at least encrypt these bits of juicy information.

So here we have an ever-growing string of attacks that seems to point to some online criminals’ rising interest in stealing and exposing usernames and passwords. Yet a long-standing and recognized company like Yahoo presumably took no measures to ensure sensitive stuff like customer account credentials were kept safe and sound – which undoubtedly will lead to a bevy of additional private goodies and surely some spikes in spam and phishing incidents.

Meanwhile, there are many organizations that have their security and risk management plans down and are constantly evolving them to account for gaps that inevitably arise. These don’t make the headlines. They acknowledge that defense in depth measures have their place and that current times dictate an acceptance that their corporate networks likely have been infiltrated by the bad guys, hence the need for newer network monitoring and other more advanced technologies and processes that provide actionable insight when culprits are found. They understand that security awareness training is cheap and, in some instances such as my hairdresser’s brother, impactful.

Large, well-known and successful companies like Yahoo, LinkedIn and others should be one of these. They set the example either way and, sadly, it’s the one not to follow.

Illena Armstrong is VP, editorial director of SC Magazine.

“Current times dictate an acceptance that corporate networks have been infiltrated...”
Rich Baich, principal, security and privacy, Deloitte and Touche
Greg Boli, global information protection and security lead/partner, KPMG
Christopher Burgess, chief security officer and president, public sector, Alpaca
Jaime Chamanga, managing director, CISO Board Consulting
Rufus Connell, research director - information technology, Frost & Sullivan
Dave Cuillinnane, chief information security officer, eBee
Mary Ann Davidson, chief security officer, Oracle
Dennis Duvalin, assistant vice president, information security and compliance services, George Washington University
Gerhard Eschelebeck, chief technology officer and senior vice president, Symphos
Gene Fredriksen, chief 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 Mathew, director, information protection, KPMG
Stephen Northcutt, president, SANS Technology Institute
Randy Sanovic, former general director, information security, General Motors
Howard Schmidt, former cyber security coordinator, White House; former president and chief executive officer, Information Security Forum
Ariel Silverstone, former chief information security officer, Expedia
Justin Somaid, chief information security officer, Yahoo
Craig Speziele, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft
W. Hord Tipton, executive director, (ISC)²
Amit Yoran, chief executive officer, Nefis; former director, U.S. Department of Homeland Security’s National Cyber Security Division
* amberus
Pakistan top producer of zombie IP addresses

For the period reported, the EMEA region (Europe, the Middle East and 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 leaders were Brazil in South America, the United States in North America and India in the Asia-Pacific region. Source: Symantec
Nearly 6.5 million LinkedIn passwords were posted online

Top breaches in June

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linkedin.com (Mountain View, Calif.)</td>
<td>A file containing easily decryptable passwords was posted online by a group of hackers.</td>
<td>6,458,020</td>
</tr>
<tr>
<td>Atkinson &amp; Co., PERA (Albuquerque, N.M.)</td>
<td>A computer containing information on employees and clients of The Public Employees Retirement Association (PERA) of New Mexico was stolen from Atkinson &amp; Company.</td>
<td>100,000</td>
</tr>
<tr>
<td>Franklin’s Budget Car Sales (Statesboro, Ga.)</td>
<td>The FTC fined Franklin’s Budget Car Sales for allowing peer-to-peer software to be installed on its network, which resulted in consumers’ personal information being compromised.</td>
<td>95,000</td>
</tr>
</tbody>
</table>

Spam

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

Zombie IPs

Global distribution

Top 5 attacks used by U.S. hackers

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

Top 5 attacks used by foreign hackers

1. ZeroAccess trojan
2. Web-based exploit kits
3. Zeus trojan
4. Sinowal trojan
5. Anti-phishing domain adviser

SMS spam

Volume by month for each region

Received spam

Top five regions

Index of cyber security

Perceived risk

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

Internet dangers

Top 10 threats

1. Salty.AT ▲ | 12.05.10 | Virus | 5 | 4
2. Lamechi.B ▲ | 01.10.12 | Downloader | 9 | 3
3. Winwebsec ▲ | 09.22.10 | Scareware | 4 | 1
4. Zbot.gen/AF ▲ | 12.16.10 | PasswordStealer | 0 | 0
5. Hotbar ▲ | 09.23.10 | Adware | 0 | 0
6. Agent ▲ | 12.08.10 | Worm | 0 | 0
7. Expir.AN ▲ | 12.03.11 | Virus | 0 | 0
8. Rehup.A ▼ | 09.21.10 | Worm | 1 | 3
10. Vrut.BN ▲ | 10.05.10 | Virus | 0 | 0
Update

2 minutes on... U.S. cyber coordinator moves on P14

Me and my job Reviewing IT auditees’ security policies and procedures P15

Skills in demand Continuity, disaster recovery specialists are needed P15

NEWS BRIEFS

Foreign companies need not apply. That’s the message the Canadian government relaid when it enacted a national security exception to bar foreign vendors from bidding on the construction of its new telecommunications system. While a trade exception is sometimes used in military procurements, it’s rare to see it invoked in civil engineering projects.

The use of the clause, which overrides trade obligations under the North American Free Trade Act and the World Trade Organization agreements, reflects the government’s belief that its communications networks have been “the target of hostile threats which causes grave concerns about the implications of cyber threats on Canada’s national security.”

In a statement circulated to IT suppliers, Public Works and Government Services Canada said it was creating a “cyber perimeter” by limiting bidding to build the new system to Canadian companies. In addition, preference will be given to suppliers who use equipment made in Canada. The new telecommunications system is the first phase of a massive overhaul of the government’s data center infrastructure.

Canada’s spy agency doesn’t usually venture into legislative affairs, but to broaden the country’s online oversight it was eager to make an exception. An Access to Information filing has revealed that the head of the Canadian Security Intelligence Service (CSIS) wrote to Public Safety Minister Vic Toews, offering the agency’s assistance to make the government’s controversial Internet surveillance bill more palatable. The bill stalled in Parliament after Toews drew the public’s ire by stating that the opposition would not support the legislation or “stand with the child pornographers.”

The government reacted to the controversy by delaying debate of the bill, but CSIS Director Richard Fadden offered to draft “potential options to strengthen the accountability regime” related to how law enforcement can obtain access to internet subscriber information.

India’s government claims it has found a way to monitor email sent via BlackBerry, something even manufacturer Waterloo, Ontario, Canada-based Research In Motion (RIM) claims it can’t do. It true, the technical discovery could end months of squabbling between India and the beleaguered Canadian phemonena RIM has long maintained that its network is so secure that it could not comply with the country’s requests to monitor BlackBerry emails. The government claims it needs the oversight to intercept messages between criminals or anti-government extremists.

India’s Information Technology Secretary Shri Chandrakashan claimed his government new believes it can monitor BlackBerry emails without decrypting the actual messages. He declined to give further details.

Along with Indonesia, India has threatened to block RIM’s access to its large, lucrative market if the company continues to refuse to provide its customers’ encryption keys. The company has maintained that it has no access to individuals’ codes.

All the news

Online collective

Anonymous took credit for hacking computer systems to yield 2.4 million emails on Syrian politicians, ministries and government-connected companies. The emails, dubbed the “Syria Files,” were released by whistle-blowing site WikiLeaks. They are said to “shine a light” on the “inner workings” of the repressive Assad regime in Syria, where violence has escalated into a civil war.

THE QUOTE

Phishing is a really old technique, but old doesn’t mean that it’s ineffective.”

—Dmitry Bystuzhev, head of global research and analysis in Latin America for Kaspersky Lab, commenting on various methods cyber criminals use to go after users of online banking.

Debate

The evasiveness of Flame may have been what prevented traditional AV technology from catching it sooner.

When Flame malware became front-page news, we went digging through our collections for related samples. We were surprised to find out that we had samples of Flame already from 2010, sent to us via automated systems. They had been classified as clean. So, we missed Flame for two years. That’s a spectacular failure for our company, and for the anti-virus industry in general. Basically, nobody detected Flame.

Flame was most likely written by a Western intelligence agency. The fact that it evaded detection proves how well they did their homework. The unfortunate truth is that traditional, consumer-grade anti-virus products won’t be able to protect against targeted malware created by nation-states with big budgets. It will protect you against the regular stuff: banking trojans, keyloggers and email worms. But protecting your systems against malware from foreign intelligence agencies requires a layered defense, with network intrusion detection systems, whitelisting and active monitoring of inbound and outbound traffic of the organization.

THE SC MAGAZINE POLL

What social media platform do you spend most of your time on?

Google+ 26.67%

LinkedIn 43.33%

Facebook 23.33%

Pinterest 1.67%

Source: Facebook

THE STATS

901m

monthly active users on Facebook at the end of March

80% of Facebook’s monthly active users are outside the U.S. and Canada

Source: Facebook

FOR

Mikko Hypponen Chief Research Officer F-Secure

AGAINST

Bruce Schneier Chief Security Officer BT

Threat of the Month

MS zero-day

What is it?

A zero-day vulnerability in Microsoft XML Core Services, which is included with various Microsoft products to provide W3C compliant APIs for parsing of XML content.

How does it work?

The vulnerability is caused by an error in the “DOMNode::get_defining_function” when the “definition” method is called for a DOM object, causing the value of a VARIANTARG to be left uninitialized. Later, this value is dereferenced as an object pointer, which allows gaining control of the program flow since it is possible to cause the stack space storing the uninitialized VARIANTARG value to contain attacker-controlled data.

Should I be worried?

The vulnerability is being actively exploited via Internet Explorer.

How can I prevent it?

Microsoft released patches for this flaw in mid-July. Previous to the release, Microsoft issued a security advisory, KB2719615, with a Fix it solution that can be used as a workaround to block the attack vector.

Source: Carsten Eiram, chief security specialist, Secunia.
U.S. cyber coordinator moves on

What does the nation’s first cyber security coordinator do for an encore on leaving government service? First, one would believe that Howard Schmidt, a 40-year veteran of the discipline, will penning another book, this one detailing the three years he spent serving in the Obama administration as the United States’ top computer security adviser. He stepped down at the end of May. One knows for a fact, however, that he has joined another book, this one specializing in data privacy and operations.  

Walter Stryszchar Jr.  
University System of Maryland

How do you describe your job to average people? I usually describe my job as a computer security and a quality control assessor. I tell people that I evaluate security, it’s less of getting into the computer system’s bits and bytes as it is reviewing IT auditees’ security policies and procedures. 

Why did you get into IT security? IT security is a field that just isn’t boring. Technology changes almost daily, and as an auditor who examines entities numerous times, there’s always new things to learn about the network, applications, operating systems and web technologies. 

What was one of your biggest challenges? Sorry, I have no stories to tell here. But, I do have an ongoing challenge wherever I audit: Convincing senior management that controls over IT are mission critical. Their buy-in is paramount to maintaining/strengthening a sound IT security program. If the big boss doesn’t think it’s important, will anyone else? 

What keeps you up at night? Not knowing who gets in, accesses information, and gets out without being detected, or who gets buried deep in voluminous audit logs. A nother concern is the thought that accessed data will someday be used to discredit or financially damage our organization. 

Of what are you most proud? I’m proud anytime an audi-tee contacts me and asks my advice on a security issue or control procedure. It’s not unlike having your teenage son or daughter come to you for advice: It doesn’t happen very often, but when it does, it’s a great feeling. 

For what would you use a magic IT security wand? I’d use it to detect every unauthorized access attempt on our systems and then send a command to the intruder’s computer that both disables it and reports the intruder to the authori- ties. Yep, that’d do it! 

Update

2 MINUTES ON...

U.S. cyber coordinator moves on

Source: MeriTalk

$12,000,000,000 could be saved off the annual IT budget if federal agencies got aggressive about the cloud

Source: LightSand

Saar Bitner, CEO, SysAid Technologies

Saar Bitner, CEO, SysAid Technologies

Wendy Rafferty, vice president of services division, CrowdStrike

Victims. Prior to joining the company in 2007, Saar was the executive director of product management for LightSand. He replaces founder Israel Lifshitz, who will remain with the company in a strategic capacity. www.sysaid.com

Wendy Rafferty has joined CrowdStrike, which offers malware assessment and inci-dent response services, as vice president of the services division. She reports to Shawn Henry, the company’s president and a 24-year veteran of the FBI. A 10-year information security vet- eran, Rafferty formerly managed Mandiant’s Western region, and before that was a special agent performing computer crime investigations with the U.S. Air Force. www.crowdstrike.com

Brandon Edwards and Aaron Portnoy, former researchers with Tipping-Point’s Zero Day Initiative (ZDI), have launched Exodus Intelligence. The company offers a bug-buying program, as well as a security intelligence service with customized infor-mation on new vulnerabilities and threats. The Exodus team also regularly gives both public and private training courses. www.exodusintel.com

Wendy Rafferty

Wendy Rafferty, vice president of services division, CrowdStrike

The two also plan to revive the Western region to drive new business to the United States as its critical IT assets, assess the costs of a potential loss, define options for their protection and plan their response. This presumes document mission- critical IT assets, assess the costs of a potential loss, define options for their protection and implement their plans.

What it takes

BC/DR positions require project management, business process and risk planning expertise.

Compensation

Salaries for BC/DR analysts range from $35k to $70k; while salaries for BC/DR planners range from $70k to $105k. 

Source: Jerry Irwin, CDO and COP of sales at Prescient Solutions, www.prescientSolutions.com

Skills in demand

Since the Sept. 11 attacks, IT business continuity (BC) and disaster recovery (DR) specialists have been in great demand and continuously growing demand. These pros document mission-critical IT assets, assess the costs of a potential loss, define options for their protection and implement their plans.

What it takes

BC/DR positions require project management, busi-ness process and risk planning expertise.

Compensation

Salaries for BC/DR analysts range from $35k to $70k; while salaries for BC/DR planners range from $70k to $105k.

Source: Jerry Irwin, CDO and COP of sales at Prescient Solutions, www.prescientSolutions.com
A recent U.S. House Financial Services Committee hearing on cyber threats affecting capital markets and corporate accounts, several industry experts detailed how cyber crimes represent a significant danger to the long-term national and economic security of the United States or any nation targeted for attack. During my testimony, I urged Congress to enhance collaboration and data sharing among the public and private sectors to ensure that all available resources are working in concert to protect and defend the financial sector. While many of the attacks launched against the sector thus far have been limited in scope, cyber criminals are increasing their technological sophistication at a rapid pace – and their attempts to initiate denial-of-service attacks on the public websites of consumer banks, credit card processors and stock exchanges have the potential to produce system-wide impacts.

The key question for the industry and policymakers is: How do we prioritize and balance risk mitigation efforts focused on preventing an attack that could damage or destroy a key portion of the financial system's critical infrastructure against the relatively low frequency to date of impactful attempts of this nature? However, before this question can be answered, consensus needs to be developed around how critical infrastructure is defined. Current law describes critical infrastructure as "systems and assets, whether physical or virtual..." The translation of this broad definition into actual "systems or assets" is an important part of the ongoing dialogue between the industry and policymakers. It is essential to determine where extra protections are needed – and just as importantly, where they are not. The definition must be narrow enough to cover the key components of the infrastructure so that investment in mitigation initiatives is properly focused. The Financial Services Sector Coordinating Council (FSSCC) is actively working to develop a process for defining critical infrastructure for the financial sector. This is a priority because recent federal cyber crime legislation leaves it to the agencies to make that determination. It is essential that the industry play a leading role in this process to help shape new federal policy.

The expectation is that this effort will create a framework for the industry to more accurately define what is critical infrastructure. It will also help ensure that the unique needs of the financial sector are identified while avoiding a one-size-fits-all approach. Most importantly, it will empower industry participants to have a greater hand in strengthening our collective defenses against cyber attack.

...defining critical infrastructure as..."systems and assets, whether physical or virtual..." The translation of this broad definition into actual "systems or assets" is an important part of the ongoing dialogue between the industry and policymakers. It is essential to determine where extra protections are needed – and just as importantly, where they are not. The definition must be narrow enough to cover the key components of the infrastructure so that investment in mitigation initiatives is properly focused. The Financial Services Sector Coordinating Council (FSSCC) is actively working to develop a process for defining critical infrastructure for the financial sector. This is a priority because recent federal cyber crime legislation leaves it to the agencies to make that determination. It is essential that the industry play a leading role in this process to help shape new federal policy.

The expectation is that this effort will create a framework for the industry to more accurately define what is critical infrastructure. It will also help ensure that the unique needs of the financial sector are identified while avoiding a one-size-fits-all approach. Most importantly, it will empower industry participants to have a greater hand in strengthening our collective defenses against cyber attack.

...defining critical infrastructure as..."systems and assets, whether physical or virtual..." The translation of this broad definition into actual "systems or assets" is an important part of the ongoing dialogue between the industry and policymakers. It is essential to determine where extra protections are needed – and just as importantly, where they are not. The definition must be narrow enough to cover the key components of the infrastructure so that investment in mitigation initiatives is properly focused. The Financial Services Sector Coordinating Council (FSSCC) is actively working to develop a process for defining critical infrastructure for the financial sector. This is a priority because recent federal cyber crime legislation leaves it to the agencies to make that determination. It is essential that the industry play a leading role in this process to help shape new federal policy.

The expectation is that this effort will create a framework for the industry to more accurately define what is critical infrastructure. It will also help ensure that the unique needs of the financial sector are identified while avoiding a one-size-fits-all approach. Most importantly, it will empower industry participants to have a greater hand in strengthening our collective defenses against cyber attack.

Mark Clancy
Managing Director and CISO for
The Depository Trust & Clearing Corp. (DTCC)

The FSSCC is working to... ...define the key functions performed within the financial sector and determine the importance of each of those functions against the impact they will generate.

Measurable assets
The council, on behalf of the financial vertical, is also quantifying how much of a sector function is performed in an individual "system or asset," says Clancy.

Targeting financial sector
Clancy says he was heartened by the level of support among members of the House Financial Services subcommittee to find solutions to the growing problem of attacks.

Keeping money flowing
The Depository Trust & Clearing Corp. (DTCC) is a non-commercial cooperative that serves as the critical infrastructure for capital markets globally and in the United States.
When hackers from the United States, Eastern Europe and Russia raided Heartland Payment Systems to funnel out an estimated 100 million credit card numbers, most observers were flabbergasted by the astonishing number of records involved in the incident.

But as it would turn out, if the Princeton, N.J.-based company had only been privy to the methods and malicious executables that the intruders used, it may have avoided one of the largest recorded data breaches in history, says John South, Heartland’s chief security officer. This may sound implausible in hindsight, except that South and his team were far closer to those answers than you may think.

“One of the things we found going through our breach, the indicators that would have been available to protect ourselves were out in [the financial services] community,” he says. “People knew about the indicators, but they had no way of sharing the information. Everything [the hackers] used, everything was known by someone at some point in time, including some of our competitors. If we had known them, perhaps things would have been different.”

The breach, which was disclosed in January 2009, prompted Heartland to not only get serious about beefing up its data security stance – it implemented an end-to-end encryption system to cloak credit card numbers from point-of-sale swipe to bank handover – but also recognizing the value of collaboration. Bob Carr, the company’s founder and CEO, helped launch the Payments Processing Information Sharing Council, part of the Financial Services Information Sharing and Analysis Center, better known as FS-ISAC. The endeavor created an interesting dynamic – all of the council’s members are staunch competitors – but it underscored the collective realization that threat data carries exponentially greater value when it is aggregated.

All of the drivers to make more partnerships like this one thrive seem to be in place. By their very nature, IT security departments crave visibility. And, they are befuddled by the sheer speed by which attacks occur and the long period it often takes to discover them. Plus, the criminals share information, so why shouldn’t the good guys, too? If everyone assisted one another, the theory goes, they’d be in a much more enviable position to combat cyber risks. Still, despite efforts across the industry to improve threat intelligence, even among seemingly fierce rivals, significant barriers to information sharing still exist, chief among them the fear of admitting compromise.

That’s why researchers at the Georgia Tech Research Institute (GTRI) are trying to reimagine information sharing through the introduction of Titan, an anonymous threat intelligence system that, for a small cost, seeks to lend a hand to organizations of all sizes. In devising the idea, engineers at GTRI determined that a need existed within the industry to communicate around threat data. Large organizations either relied on purchasing too many appliances for malware analysis – or they had to build their own – while smaller outfits didn’t have the budget to do either. Yet most companies, no matter...
their spending ability, have one thing in common: Their security efforts are far too inward focused. “A lot of them think of this as their dirty laundry,” says Christopher Smoak, a research scientist at GTRI and one of the creators of Titan. “It’s time for us to stop being so secretive about even the stuff we know about. I bet if we’re not going to start building these bridges to share stuff with each other, then we might as well give up.”

He even suggests sharing intelligence directly through IC3, or when organizations often are most reluctant, like during internal investigations, or, if they are permitted to, during a law enforcement probe. The more, the better, Smoak believes.

**Titan of industry**

There are already an abundance of efforts underway to share information, from Small I d s i t s among a few trusted parties to nonprofit efforts like the Shadowserver Foundation to industry associations like F5-ISAC to for-profit threat intelligence vendors like Microsoft or VeriSign’s iDefense Security Intelligence Services. Even the U.S. government is trying to get in on the game through the introduction of a number of bills in Congress, such as the controversial Cyber Intelligence Sharing and Protection Act (CISPA), which would regulate information sharing among the public and private sectors.

The key differentiator with Titan is accessibility and interaction, Smoak says. The portal is billed as a “community-driven” threat intelligence engine, operated by an entity with no cards in the game. It already has support from close to 20 organizations in industry and government, is receiving and processing more than 100,000 malware samples each day, and is scheduled to officially go live by the end of the summer.

Smoak admits that the portal will still be work for reporting and retrieving information about mass malware, rather than more targeted threats, because that is what organizations are more likely to fess up about.

“Members can search malware samples based on industry, specific network domains and even develop and share their own analysis module,” according to a fact sheet. “Titan users may quickly and easily pass samples of both known and unknown type to the system, which automatically processes them according to file type and user request, and produces dynamic reports within minutes. Unlike traditional malware-analysis platforms, Titan does not define a static set of analysis methods. Instead, the framework allows members to add, remove and modify ‘pluggable’ analysis modules to suit analysis needs over time.”

The researchers believe a big draw will be the portal’s versatility. “Whether an engineer is one who wants to see the results of analysis or a researcher who desires high-level reports of some activity across a particular vertical, they can all extract value. “We’re adaptive,” says GTRI research scientist Andrew H. Ward. “We’re flexible. The advantage Titan has is that as threats change, we can change at the same speed. You don’t have to buy a new appliance.”

Heartland’s South says systems like Titan provide help to counteract some of the pressures organizations are facing, such as an overworked security staff and small budgets, which have worked to tip the balance even more in favor of the attacker. “It gives us insight into the things we should be looking for,” he says. “For example, by someone making a DLL [dynamic-link library] available to us as an indicator, we could look at our network to see if that DLL exists somewhere.”

John Johnson, the global security program manager at Illinois-based John Deere, the world’s leading producer of agricultural machines, says he sees the value in Titan’s drive to cross-pollinate threat intelligence across industries. “That’s because the manufacturing sector in which John Deere plays traditionally has been slow to embrace the latest security and technology and doesn’t have the formalized sharing infrastructures that the more heavily regulated verticals do. Instead, Johnson relies on data sharing within a CISO peer circle to which he belongs in the Chicago area. “It’s basically a dinner group where we get together and talk in person,” he says.

But, he recognizes that malware and the techniques used to spread it often are agnostic of industry. “It no longer is anyone immune. ‘We can’t rely on obscurity and lying low and waiting for the financial companies to take a lead,’ Johnson says. “I think we need solutions that are more intelligent and more proactive. If academia can step up and pull people together and demonstrate it’s going to work and these concerns are being addressed, I think it’d be a worthwhile approach.”

**Roadblocks to acceptance**

The “concerns” Johnson speaks of are ones Smoak often hears. A big one for Johnson is trust. “That’s why a critical feature of Titan is its anonymity component to prevent any leaks that could jeopardize an investigation or encroach on someone’s privacy. Or provide fuel to the very attackers Titan is seeking to stop.”

Smoak and company have extended a great deal of effort in ensuring that Titan is leak-proof, and that its members are vetted to ensure that information isn’t accessible to the sinister.

“Every time data goes in or out of the system, we perform pre- and post-filtering that strips out things folks can’t see,” he says. “That’s before it leaves our internal network. Additionally, all data associated with a user/organization is referenced by a pseudo-random identifier. The hope, though, is that once contributors feel comfortable using Titan, they will de-anonymize themselves and pick out certain people with whom they want to work. This speaks to Titan wishing to solve a more fundamental problem: removing the stigma that a successful compromise should be cause for shame.

As for vetting users, Smoak says: “We call or have a face-to-face meeting with every prospective Titan member. During this call, we discuss background on the requesting user/organization, as well as give information about our background.”

For Titan to succeed, it also will have to convince ardent critics, such as John Pescatore, vice president and research fellow at Gartner, who says information sharing has amounted to more of a buzzword than a saving grace. To make his point, Pescatore references anti-virus companies, which, he says, essentially have been doing threat intelligence collaboration for better than two decades. Oftentimes, a business customer submits a malware sample to an AV firm, and the vendor in turn creates a signature. “The answer to these attacks is not going to come from more information sharing,” he says. “If that was the case, anti-virus would’ve solved our problems a long time ago. The answer is making your systems less susceptible to attack.”

But, Smoak says Titan offers far more capability as an information repository than an AV company can provide. “AV vendors typically only provide signatures to their particular product,” he says. “This means that during the time it takes the AV vendor to get a signature back—which may not necessarily detect all variants or other dropped files—malware may have already moved laterally or downloaded additional code that has not been identified. Their financial motivations only serve to push a small AV signature update and nothing else, which leaves organizations in a bit of a bind when remediating something in a time crunch.”

Pescatore makes a fair point, though, when he says that any successful data-sharing endeavor necessitates a two-way street. Naturally, most organizations want to get more than they give, and any model would be hard pressed to achieve the inverse of that. But mutual contributions are being addressed, I think it’d be a worthwhile approach.”

The researchers believe a big draw will be the portal’s versatility. “Whether an engineer is one who wants to see...
Polish-born Canadian Rafal Rohozinski parleys his nonprofit initiatives exploring the internet’s shadier regions into a for-profit business. Danny Bradley reports.

Rohozinski pioneered the Kiev Freenet – the first free access internet point in the Commonwealth of Independent States (CIS), made up of former Soviet republics – and helped to develop a business centre attached to the project.

One of his strengths, say those who have worked with him, is his ability to straddle the technical and political worlds. “He’s good at working in a multi-cultural environment,” Browne says.

The ability to bridge communities was crucial. Browne recalls conversations with UN bureaucrats in New York who knew nothing about the institution’s work in the Ukraine. Browne would direct them to a website, and they would look at him nonplussed. “We were at the cutting edge of a major change in the UN, but we almost got caught out by our own cleverness,” Browne says. “People didn’t know how to find URLs.”

Rohozinski’s success in Kiev led to further travels. Throughout the 1990s, as part of the UN’s development program, he was sent out to build networks across Asia and the CIS.

In the early 2000s, he was bought back to help set up the Advanced Network Research Group, part of Cambridge University’s Cambridge Security Programme, a post-9/11 initiative designed to help address security concerns around the world.

“Around this time, the Ford Foundation, which works with ‘visionary leaders and organizations to change social structures and institutions’ – plucked Rohozinski from among five academics, including Ron Deibert, the director of the Canada Centre for Global Security Studies (he also heads up the Citizen Lab at the Munk School of Global Affairs at the University of Toronto). The foundation gave the two funds to look at how technology changed society.

The two men shared a passion for cyber space governance, and set up the Open Network Initiative (ONI) and the Infowar Monitor. Both served to document and expose the control of information in areas prone to censorship.

The two also collaborated on Psiphon, a tunnelling system to help get information past internet censors, which is now used to send content from Western nations into regimes that would prefer it blocked. Rohozinski is the group’s CEO.

He is happier at the raggedy edges of the internet than at its core. His work has taken him to many places, including Palestine, where he served from 2005-06 as chief technical adviser to the Palestinian Authority, and to other regions, including Lebanon and the Congo. (He also spent time in Rwanda and Nigeria while he was the research director of the Small Arms Survey, a group he co-founded in 2000.)

And, along with Muggah, Rohozinski created The Open Empowerment project, a collaboration with the Igarapé Institute, supported by Canada’s International Development Research Centre, which explored how cyber security issues play out across Latin America.

Rohozinski’s nonprofit information security research goes beyond the Americas. He has published reports covering everything from the Chinese Ghostnet network, a large cyber espionage enterprise detected in March 2009, to the broader use of cyber spying. Muggah published the “Global Burden of Armed Violence” report in 2008 and 2011, and a number of studies on violence around the world, and cites Rohozinski and Deibert, the woman to whom he is married, for instigating this work.

Some projects naturally come to a close, however, as the goals of Rohozinski and his collaborators shift. For example, the Infowar Monitor, the project that he set up with Deibert to explore information warfare, ended in January. Rohozinski says his more commercial activities and work for government clients pull him away from the academic world.

“There is a philosophy to take it into more of an academic setting,” he says referring to Deibert and the Munk Centre. “Ron is now a full professor at the university, and he felt more comfortable taking a normative stance. He has a strong posture on issues of surveillance, and it became more difficult for him to be engaged with a group that works with the government on these issues.”

“The difference is this,” adds Rohozinski. “I work with law enforcement and Public Safety Canada.” And while he acknowledges mistakes in policy and public communication, he is forgiving. When, during government debates over lawful-access legislation, Canadian ministers told the public that they were either with the government or with the pedophiles, it was a mistake, he says. Nevertheless, he adds: “I understand there are institutional growing pains.”

Once again, then, he finds himself pivoting between different communities: technological, political and academic. Perhaps some amicable shifts were inevitable.

“We still collaborate, but we’re not standing shoulder to shoulder in the way that we were in the past,” Rohozinski says of Deibert.

As in cyber space, relationships and boundaries in the community focusing on governance tend to ebb and flow.
We exist in a digital age. The exponential growth of the digital reality that surrounds and governs our lives can be quantified by the rate at which the volume of digital information in the world continues to expand.

Not so very long ago – 2009 to be exact – it was reported that the total volume of digital information in the world was 0.8 zettabytes (ZB). Within 12 months that figure had become 1.2ZB. It is forecast to become 35ZB by 2020. This digital information exists around the globe and much of it is accessible from more or less anywhere in the world, from any mobile or static device.

Information isn’t just something that sustains us as individuals and businesses, it has become a high-value asset not only for those to whom it belongs, but also a high-value target for those unsavory characters who seek to use it for criminal gain – to disrupt business, steal data, overwhelm systems and coordinate cyber crimes.

In a purely business context, information assets are what distinguish one organization from another, they define and maintain competitive advantages, they can determine success or failure, they make corporate organizations unique from one another.

That’s why the security of both personal and corporate information assets has become an absolute priority that has fuelled the growth of the global information security industry and made it one of the most dynamic and fastest-moving markets ever.

Of this zettabytes-worth of data that shapes our personal and business existences, a significant proportion of it is ‘software,’ which can be more specifically defined as legitimate (clean) software, known malicious software (viruses, trojans etc.) and unknown (grey) software.

An incident involving a single piece of malicious software or ‘malware’ incident can potentially lead to the loss of highly valuable corporate information assets and cause widespread disruption to business systems and business processes costing not just thousands, but potentially millions of dollars in remediation costs and lost business.

The battle between malware authors and the security technology industry is forever escalating. For many anti-malware technology developers, it is practically impossible to stay ahead of all threats, particularly newly emerging zero-day threats, which can spread worldwide within hours.

The scale of the problem that users face is summed up by the fact that in 2006 a new piece of malware was being discovered every minute. Nowadays a new malware sample is found every 2 seconds! Kaspersky Lab for instance, is currently identifying around 70,000 malware samples every day of which around 50% are new, malicious. Given the current scale of the problem, who knows what the volume of malware-related problems will be when we hit the 35ZB of digital information in 2020!

Anti-malware technologies are based around a number of diverse approaches including signature-based detection and heuristics; however, as authors of malware are finding more innovative ways to circumvent these types of detection, a new approach is being implemented by some companies which consider the problem from the opposite end of the protection spectrum.

Whitelisting – and Application Control.

Technically, whitelisting is a huge database of clean and trusted software that is regularly updated.

So, as cyber criminals continue releasing new malware day in, day out, users who make use of a file reputation service should be reliably informed about what can be run with no worries, and what it might be better not to run.

Application control is the technology that facilitates the use of a whitelisting database in a corporate network. It includes features such as restricting application startup and managing application privileges and checking applications for vulnerabilities.

The default deny mode is potentially an integral part of application control technology and is a particularly effective method of protection against malware incidents given that it prevents the launch and spread of malicious software. Effective, it blocks the launch and execution of any software which is not on the whitelist and which has not been clearly identified as secure by the administrator.

It’s potentially a major opportunity for the security industry to at last be one step ahead in the battle with cyber criminals and for users to have an additional layer of protection against unknown, zero-day threats.

Therefore, the business impact of this new way of dealing with malware threats could be significant. As Gartner has pointed out*: "Vendors must combine proven anti-malware tools, data protection capabilities, and new technologies such as live reputation database lookup and whitelister to provide customers with effective, manageable protection on a growing variety of traditional and emerging endpoint platforms.

*Source: Gartner, Endpoint Protection Platforms Blending Security, System Management, and Data Protection, Application Control and Whitelisting for Endpoints, 10 March 2011
“Default deny application control and whitelist systems, however, offer some game-changing protection potential versus blacklisting solutions. Default deny whitelist puts endpoints into a stronger defensive posture by preventing any software not explicitly allowed by policy from installing or launching.”

Putting Application Control and Whitelisting to the Test.

Application control is not really anything new, but the technology has only just started to be built into comprehensive, all-in-one security solutions. Kaspersky Lab recently commissioned West Coast Labs to independently carry out some comparative performance tests on a number of leading security solutions.

West Coast Labs developed a universal methodology with over 40 test cases simulating the usage of whitelist and application control technologies in real-life situations. A special system of weighting was applied in order to properly evaluate the quality of feature implementation in every case. In total, seven vendors were invited to participate in the testing, although three (Lumension, Bit9 and Coretrace) declined.

Those that participated in the tests were:

- Kaspersky Endpoint Security 8 for Windows managed by Kaspersky Security Center, corporate security solutions from Symantec (Endpoint Protection 12.1) and McAfee (Solidcore Application Control 5.20 with ePolicy Orchestrator 4.6).

The test results were presented as percentages of a theoretical maximum score. The final result for Kaspersky Lab’s solution in application control testing was 91%, while the next best solution achieved just 81%. The third vendor scored 56%. The average score in this evaluation was 76%.

The default deny scenario implementation was tested separately and Kaspersky Lab’s solution was awarded a 100% score, based on the accuracy of the whitelisting database contents and the level of manageability of the application control policies and administration rights. The solution from the second best vendor got 85%, and third vendor got 37%. The average score in this testing was 74%. A total of 20 test cases were used in this evaluation.

The comprehensive report and an executive summary for the application control and default deny scenario testing is available from the West Coast Labs website at www.westcoastlabs.com/producttestreports/

<table>
<thead>
<tr>
<th>TEST RESULTS</th>
<th>Total available</th>
<th>Weighted roll up scores, percentage fulfillments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaspersky</td>
<td>Vendor A</td>
<td>Vendor B</td>
</tr>
<tr>
<td>Whitelist Creation</td>
<td>1740</td>
<td>740, 100%</td>
</tr>
<tr>
<td>Whitelist Compilation</td>
<td>600</td>
<td>600, 100%</td>
</tr>
<tr>
<td>Application Control Policies Management</td>
<td>280</td>
<td>280, 100%</td>
</tr>
<tr>
<td>Granular Control Policy Management</td>
<td>600</td>
<td>600, 100%</td>
</tr>
<tr>
<td>Whitelist &amp; Application Control Administration Rights Management</td>
<td>240</td>
<td>240, 100%</td>
</tr>
<tr>
<td>Event Monitoring and Reports Audit</td>
<td>410</td>
<td>410, 100%</td>
</tr>
<tr>
<td>Managing Whitelist and Application Control</td>
<td>190</td>
<td>190, 79.9%</td>
</tr>
<tr>
<td>Overall Scores</td>
<td>3230</td>
<td>2924, 89.8%</td>
</tr>
</tbody>
</table>

Table 2.0 – overall scores for each area
With more than 100,000 employees, Cisco Systems has embraced the bring-your-own-device (BYOD) phenomenon, defined as the burgeoning penetration of personal smartphones, tablets and laptops into the workplace.

Steve Martino, the company’s vice president of information technology, says almost 60 percent of Cisco employees have at least one mobile device connected to IT services, not including laptops, and more than 15 percent have more than one handheld that they use for job responsibilities. In terms of the benefits of deploying such an environment, the costs saved by Cisco for not issuing the devices itself are last on Martino’s list, which may be surprising to some.

Instead, employee productivity and engagement take the lead, he says. “Users who have the freedom of choice to bring their own device, are seeing about 30 minutes a day [of] greater productivity than those that are using devices they’re not comfortable with,” Martino says. “I think it’s comfort, it’s familiarity and it’s also time and place. When and where they can use their device. Those are the two drivers.”

Like at Cisco, many enterprises around the world are finally taking note of the advantages that mobility adds to their business. By now, security professionals are quite familiar with the BYOD term, and while the wave of mobile devices flooding the workplace wasn’t initially welcomed with open arms by those charged with protecting enterprise networks, it seems as though organizations at every level believe there’s no choice at this point but to embrace it.

Many concerns revolve around the additional points of entry available for cyber criminals, increasing the likelihood of sensitive data extraction or creating disruptive scenarios that could be extremely costly for enterprises. And, with looming threats and an increasing number of threat vectors, security pros are faced with a big decision: to lock down or not to lock down. There are pros and cons, many say.

Threats are always present no matter which type of environment is deployed, says Lawrence Reising, general manager for mobile security at McAfee, an Intel-based data security firm. He says it’s only a matter of time before enterprises have to step up to the BYOD challenge at hand.

“At this point, I’d say that a significant proportion of enterprise and government organizations have adopted that BYOD is here now and is inevitable,” Reising says. “They assume that it’s necessary for organizations to support employee-owned devices.”

A multilayered approach

BYOD adoption consists of a multilayered security approach that includes protecting the content on the device, since the apps host a majority of the vulnerabilities, he says. “The apps are what do the violations of privacy or the mismanagement of username and passwords,” Guerra says. “They present the way to break into the corporate server, not the device itself.”

Although mobile device management (MDM) software and mobile app management (MAM) solutions can block any app an administrator deems is unsafe, Guerra says it’s difficult to determine which is benign and what is unsafe. “Companies need the ability to be able to differentiate by job role, then be able to categorize those apps,” he says.

“W hat’s driving the consumption of these devices is not how cool the device is, it’s how many apps the device can play,” he says. Thus, the security focus should be geared more toward the apps, rather than the device itself, since the apps host a majority of the vulnerabilities, he says.

“[The apps] are what do the violations of privacy or the mismanagement of username and “By having a culture that is heterogeneous, we’re facilitating a whole market here for innovation opportunity.”
MEASURING SUCCESS

Gauging performance does not necessarily result in enhanced security, but quantifying risk is still vital, reports Stephen Lawton.

These days, it seems everything has a metric. Some questions with quantitative results can be answered easily – such as how a network is performing – and key performance indicators (KPIs) can be useful in that environment, says Gartner research director Anton Chuvakin.

KPIs are a strategy to measure the effectiveness of an enterprise, a division or individual employees. However, there are other questions around basic data security that cannot be so easily assuaged. For instance, a company that spends a lot of money on security might identify attacks, but that does not mean it is well protected, Chuvakin says.

It could mean that even with a substantial security budget, the organization’s security team is not identifying and defending against the attacks. Likewise, a company with a small security budget might have an effective security plan in place that protects its corporate assets. Clearly, Chuvakin says, a security budget alone is no real indicator of how well an entity can protect its intellectual property. He maintains that because each company has its own security profile, there can be no standard set of KPIs to determine security.

A whitepaper produced by U.K.-based Iris Accountancy Solutions, a software and services company, says KPIs vary by department, so it is important for each to outline and work to its own set of measurements. The paper describes them as objectives or goals that can be used to measure the performance of each department.

KPIs generally have five qualities: they are specific, measurable, achievable, realistic and timely, according to Iris. They need to quantify issues that will make a difference, and are thus focused on areas for which the department or employee can have an impact. Creating a goal that is outside the scope of an individual or department is unachievable, and should not be considered a KPI.

As with so many aspects of managing information security, administrating data overload can be an issue, the whitepaper explains. Understanding what needs to be analyzed and putting that data into a comprehensible format is critical. Because Iris has a large number of financial services clients, a popular format is the spreadsheet, which can incorporate both current and historical data.

This leads to the inevitable question: Can one create KPIs for security? The short answer is yes and no, Chuvakin says. If one sets their standards too high, they will never reach them. Too many variables and an ever-changing security landscape mean that KPIs that are too general cannot be met.

On the other hand, if the KPIs are set at the tactical, instead of a more strategic, level, it is possible to meet those levels. The result, however, might not meet the real security needs for the network, he says. Today, setting network security KPIs is an inexact science with too many variables, Chuvakin says. “There is no silver bullet.”

With a given amount of money allotted for security, a company may spend that on specialty products based on price, he says. However, if a company takes a more holistic view of its security profile, they might find more efficient ways to protect their network – with the budget being built to meet the network’s needs rather than those of a preset spending plan.

It all comes down to determining a company’s risk profile, experts agree. Once a company understands its risks, it can start to compile the indicators to determine where potential vulnerabilities lie.

Typically, an organization’s measurable security level is related to the amount of negative incidents detected, such as the number of viruses inoculated or number of breaches halted, says Shawn Chaput, executive consultant at Privity Systems, a security consultancy in Vancouver, British Columbia.

“This approach tends to exclude the nasty stuff, such as unidentified viruses, like Flame, which was in the wild for [an estimated] two years before it was discovered,” he says. “The problem with this approach is that it tends to reward organizations for not having attributes that respond to its security controls.”

Chaput says many companies do not know that they already have been compromised because they do not have the tools or expertise to recognize what is happening on their networks. “Valuable security measurements should likely be tied to the typical C-I-A triad: confidentiality, integrity and availability,” he says. “Whatever systems are in place to protect those elements should have metrics which are measured and benchmarked. This isn’t as easy as you’d expect.”

A component to determining what is a sufficient security KPI entails defining what is and what is not a threat, Chaput says. Not every vulnerability deserves the same level of risk mitigation, just as every piece of data has its own value.

“Ultimately, an organization needs to identify its critical assets and apply security controls to those systems commensurate with the risk,” he says. “[If for example,] if an organization’s revenue solely relies on an e-commerce system, that e-commerce system would be mission critical relative to the internal SharePoint site.”

This also means that vulnerabilities that may affect that system should be treated with higher urgency than the same flaws that may affect the Sharepoint site, he adds. “Effectively, this goes back to risk-ranking methodologies with risk as a function of impact – in this case, related to criticality; probability – how likely is this to happen; and some other elements depending on the risk-ranking method one chooses,” he says.

KPIs need to be tied to the strategic objectives and the key risks and challenges of any business, says Bernard Marr, a U.K.-based management consultant and author. “It is then important to identify the questions and information needs in relation to each of the strategic objectives and challenges.”

Once the questions are clear, he says, indicators can be developed to help answer them. “Like with most strategic objectives, they are unique to any given business and, therefore, the KPIs have to be uniquely designed to answer the questions of any given business – same for security,” Marr says.

Torsten George, vice president of worldwide marketing and products at Agillicia, a risk management vendor, agrees. “A vulnerability in and of itself does not represent any risk,” he says. A risk requires a threat plus a vulnerability. “If the threat is not capable of exploiting the vulnerability or cannot reach the vulnerability, there is no risk,” he says. Once an organization has determined that the combination of threats and vulnerabilities poses a risk for the business, then it must decide how to mitigate the risk.
Who will receive recognition at the 2013 SC Awards U.S?

Your company

Your Rivals

The battle begins now. Make sure you’re a part of it.

MORE INFORMATION

THREE NEW CATEGORIES:

Best Customer Service
Best Emerging Technology
Best Cyber Security Higher Education Program

Nominations close Friday, Sept. 7, 2012
Visit awards.scmagazine.com to download your entry kit today.

Pervasive protection

All it pervasive, ubiquitous or whatever, the fact is that today’s threats are everywhere and of just about every type one can imagine. Add a semi-permeable perimeter, throw in a dash of hacktivism and you have a pretty nasty brew.

Ever before has the concept of defense-in-depth been more important as a guiding principle and been so difficult to achieve the blanket protection that the enterprise – especially the large enterprise – needs.

I have said many times in these pages that data is the key issue. If we didn’t need to protect the data we wouldn’t need network security. If we could just encrypt everything everywhere, we’d be good to go and life would be easy. That would be way too simple. As should be fairly clear, the focus is on the perimeter – or what’s left of it – and the data. But there is one more piece that deserves our attention: the endpoint.

In our Group Test, we are examining endpoint security and there are a few surprises in store. Endpoint security today is responding to the needs of the enterprise in ways it has not in the past. That’s very good news because we are inviting outsiders into our networks under what we expect to be tightly controlled conditions more and more.

Our First Look this month (click on scmagazine.com) addresses the issue of authenticating to the cloud. This is an interesting product that solves a real problem in a creative way. We were impressed by this developer’s approach to dealing with software-as-a-service (SaaS) applications in the cloud that did not have a prebuilt/defined interface to its system.

There is a movement today that says, essentially, “Throw out defense-in-depth. It’s an outdated concept.” There is some merit in the argument since we must assume that our enterprise has been breached whether we know about it or not. Given that, the naysayers argue, defense-in-depth is a waste of time. My position is exactly the opposite.

Yes, the 100 percent breach probability is likely a safer assumption than figuring that we can keep the bad guys out. Today, we are more concerned about keeping them from doing us harm once they are inside. So why would we not need defense-in-depth to do that? After all, it’s all about the data and protecting it on multiple levels seems appropriate. Sounds a lot like defense-in-depth to me.

— Peter Stephenson, technology editor

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 1548) as a basis for the test plan. Group Test reviews focus on operational characteristics and are considered at evaluation assurance level (EAL) 1 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria speak.

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

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

What the stars mean

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

★★★★★ Outstanding. An “A” on the product’s report card.
★★★★ Carries out all basic functions very well. A “B” on the product’s report card.
★★★ Carries out 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 shone in a specific area.
Lab Approved is awarded to extraordinary standouts that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

Pervasive protection

Kaspersky
A feature-rich management platform
P44

GFI
Configurable tool with granular controls
P37

Symantec
A full suite of protection that’s easy to install
P48

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

How we test and score the products

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

We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 1548) as a basis for the test plan. Group Test reviews focus on operational characteristics and are considered at evaluation assurance level (EAL) 1 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria speak.

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

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

What the stars mean

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

★★★★★ Outstanding. An “A” on the product’s report card.
★★★★ Carries out all basic functions very well. A “B” on the product’s report card.
★★★ Carries out 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 shone in a specific area.
Lab Approved is awarded to extraordinary standouts that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.
Endpoint security

In today’s more evolved enterprises, all of the endpoints are managed and coordinated through a single point. However, there are some surprises in the marketplace, says Peter Stephenson.

Kaspersky Endpoint Security 8 v8.0 is feature-rich, contains a strong management platform and is an excellent value for the money. This one is our Best Buy.

DeviceLock Endpoint DLP Suite offers full control over endpoints with native snap-ins for Active Directory management consoles. It’s a very strong offering with a good DLP feature set. We make it our Recommended product.

PICK OF THE LITTER

Kaspersky Endpoint Security 8 v8.0 is feature-rich, contains a strong management platform and is an excellent value for the money. This one is our Best Buy.

DeviceLock Endpoint DLP Suite offers full control over endpoints with native snap-ins for Active Directory management consoles. It’s a very strong offering with a good DLP feature set. We make it our Recommended product.

One of the things that we note from time to time is the mass evolution of a particular product type. To be sure, there are always those innovators that seem to be constantly updating their products to stay current – or ahead if they can – with the state of the art, but it is not all of the time that an entire product type generates a sea change. The architecture – and especially the security architecture – of the current generation of enterprise is evolving rapidly, perhaps more rapidly than in the recent past. That puts stress on security management for those networks.

If we add such things as cloud computing, SaaS (and today that could mean software or security as a service), and a semi-permeable perimeter, things quickly start getting complicated. As we mentioned in the section opener this month, we are now faced with a strong argument – stronger than in the past – for defense-in-depth. Let us give too much credit to those who believe that because we must assume 100 percent compromise of every network, defense-in-depth no longer is the answer, the facts suggest that it is, in fact, the only practical solution to securing the enterprise.

Today, though, securing the enterprise is as much about keeping the bad guys out as it is about keeping the data in. When the demarcation of a network is indeterminate, we really have no choice but to protect the data no matter where it lies. That is, at least in part, exactly what this month’s product group is all about. Taking up the slack where the perimeter defenses are ineffective and managing the data from the endpoint.

In years past, the emphasis on endpoint security was specifically the safeguarding of the endpoint itself. This year, we found that the paradigm has shifted to an enterprise-centric model where all of the endpoints in the enterprise are managed and coordination through a single point, such as Active Directory, the rule rather than the exception. Markets are maturing toward the same sort of model as most other enterprise-class security products: policy-driven tasking, management and configuration.

Many of the products we tested required an agent – which communicated with a management console – but a few use a very lightweight service. Services can be – but are not necessarily – a much smaller footprint in the device’s memory. They are more efficient, more reliable and easier to install than applications. When these agents are tied to something, such as Active Directory, they can leverage existing user groups and organizational units, thus adding to their manageability.

Since a big part of information security today involves preventing data exfiltration, this approach helps keep the data where it belongs: inside the enterprise. By deploying, for example, data leakage prevention both at the perimeter and at the endpoint, data exfiltration at the endpoint using a CD or thumb drive – devices tied directly to the endpoint and not passing through the security perimeter – can be controlled. Additionally, malware that enters the system without passing through the perimeter – carried in on a thumb drive, for example – can be detected and, again, reported centrally.

Overall, we found this set of products to be a good example of the market responding to new threats and new network architectures, both of which necessitate fresh thinking about how we protect our data.

The products in this month’s test were noticeably more mature, more feature-rich and more tightly integrated with the enterprise security architecture than in previous years. We also found that attrition due to companies going out of business or being acquired was not as prevalent for this group as it is in many other product classes that we have looked at over the past year. Already, many endpoint products are part of an integrated whole that includes both perimeter and endpoint defenses and ties all of the pieces together through a central console and Active Directory or its ilk. For enterprises of just about any size, but especially large ones, this is good news, indeed.

<table>
<thead>
<tr>
<th>Specifications for endpoint security tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Group</td>
</tr>
<tr>
<td>Provides access control to removable media</td>
</tr>
<tr>
<td>Provides access control to files and folders</td>
</tr>
<tr>
<td>Provides whole disk encryption</td>
</tr>
<tr>
<td>Provides file and folder encryption</td>
</tr>
<tr>
<td>Provides endpoint firewall</td>
</tr>
<tr>
<td>Provides endpoint AV and malware protection</td>
</tr>
<tr>
<td>Compatible with Windows endpoints</td>
</tr>
<tr>
<td>Compatible with Mac endpoints</td>
</tr>
<tr>
<td>Compatible with Linux endpoints</td>
</tr>
<tr>
<td>Preconfigured regulatory compliance templates</td>
</tr>
</tbody>
</table>

Lambrion Endpoint Management

Mifile Total Protection for Endpoint

Novell Endpoint Protection Suite v12.2

Quartet Technologies Protect De v12.7

Sophos Endpoint Protection v9.0

Symanec Endpoint Protection v12.3

Trend Micro Enterprise Security for Endpoints

Wave Systems EMBASSY Remote k5

| Provides access control to removable media | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
| Provides access control to files and folders | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
| Provides whole disk encryption | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
| Provides file and folder encryption | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
| Provides endpoint firewall | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
| Provides endpoint AV and malware protection | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
| Compatible with Windows endpoints | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
| Compatible with Mac endpoints | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
| Compatible with Linux endpoints | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
| Preconfigured regulatory compliance templates | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● |
Check Point Endpoint Security

Endpoint Security from Check Point offers up a lot of functionality that can be customized for the needs of the environment. This product is comprised of a base system, which can be supplemented with various components to suit a customer’s needs. These add-ons are referred to by Check Point as Software Blades and they include Full Disk Encryption, Media Security, Remote Access, Anti-Malware and Program Control, WebCheck, and Firewall and Compliance Check. Each one of these modules can be purchased separately or the entire set can be purchased as a full suite.

Installation and deployment was quite easy, but it did require quite a few steps. The initial deployment is comprised of deploying the Endpoint Security Server and management console and then deploying the Endpoint Security clients to all the machines on the network. We found the initial deployment to be simple and straightforward. We noticed that if other Check Point products already were running in the environment – such as a security gateway VPN, a DLP product or a Document Security product, among others – this offering can work alongside them and be managed directly using the Check Point Smart Console.

As for functionality, this product has a lot of features and functions. When fully loaded, Check Point Endpoint Security can fully control endpoints to ensure security compliance. Some of the available functions include encryption enforcement of both hard disks and removable media, firewall policy enforcement, malware detection and removal, application control to ensure unauthorized applications are not running in the environment, and web security, which allows for protection against web-based threats.

Documentation included a full administrator guide. This featured all information for the product from initial installation and deployment to configuration and use of features. We found this to be well-organized and to include many clear, step-by-step instructions, but there was a lack of screen shots and diagrams. We would like to see more visual illustrations throughout the manual as these can be helpful when learning how to use a new product.

Check Point offers a first year of full support as part of the initial purchase prices of its product. After the first year, customers can purchase additional support at various levels on an annual basis. Basic support offered includes nine hours a day/five days a week phone and email technical support, as well as access to online chat and remote support. Customers also can access a support page via the website that offers many support resources. Customers wanting 24/7 support can upgrade to a higher level.

We found the pricing structure for this product to be quite reasonable. The initial cost starts out at $60 per seat for the base system, but based on volume this price can drop down to around $30. After the base, the various blades can be added at a cost of between $6 and $20 per seat per blade. However, there is also an option to buy all of the blades at a package price of $30 per seat – bringing the total package cost to a starting price of $90 per seat for the whole suite. While this may sound pricey, we find that there is a lot of functionality in the full suite and volume discounts are available.

DeviceLock Endpoint DLP Suite

The Endpoint DLP Suite from DeviceLock offers full control over devices, peripherals and ports throughout the enterprise. Using Endpoint DLP (data leakage prevention), administrators have a vast amount of access control over peripheral ports, removable media devices, as well as network and application protocols. This ensures that only authorized devices, such as USB flash drives, microSD cards and other types of media, are used in the network and only authorized users can use said devices preventing data leakage and other compliance problems.

Installation and deployment was quite straightforward. The initial implementation was comprised of installing the enterprise server somewhere in the environment. The server software itself was lightweight and installed on pretty much any machine. Once the server was installed, the DeviceLock service was deployed quickly to client machines either through Active Directory Group Policy or by using the Endpoint DLP management console. With the service deployed, all endpoints throughout the enterprise were managed natively using Active Directory Group Policy.

The Endpoint DLP Suite features a native Active Directory Group Policy Microsoft Management Console snap-in, so administrators can modify policy and configure options using the existing group and organization unit structure already in place. The snap-in itself provides a lot of configurable options including port management, encryption requirements, application protocol controls and auditing options. We found this product to be quite simple to manage and configure overall. We really liked the approach of tying policy directly to Active Directory for added ease of use and management.

Documentation included a quick-installation guide, as well as a full administrator manual. The short quick-installation guide provided a brief overview of the suite’s components and how they are deployed, while the administrator manual provided full in-depth instructions on installation, deployment, configuration and management of the product. We found the administrator manual to be well-organized with easy-to-follow, step-by-step instructions and a lot of screen shots, diagrams and configuration examples.

DeviceLock offers customers the first year of support as part of the initial cost of the product. After the first year, customers can purchase additional assistance as part of a contract. Support offered by DeviceLock includes eight-hours a day/five days a week phone-based technical help and 24/7 email and web-based aid. Customers can access a large web-based area, which includes many resources, such as a FAQ section, user forum, support ticket request form, webinars, video demos and product documentation.

At a volume discount price of $40/perpetual license per seat for 1,000-plus endpoints, this product may seem a little on the expensive side, but we find it to be an excellent value for the money. The DeviceLock Endpoint DLP Suite comes complete with a lot of configurable options and a great amount of flexibility and control that make it simple to deploy, configure and manage. The added ease of management through Active Directory alone makes this product easy to deploy in almost any environment with little effort from administrators.
ESET Endpoint Security

ESET Endpoint Security from ESET focuses on malware prevention and overall system security to mitigate threats throughout the enterprise. This product is powered by the same engine that is used in the ESET NOD32 anti-malware client and extends functionality to the enterprise environment. ESET Endpoint Security also features full, client-side anti-spam, firewall and web content filtering and management. This allows administrators to easily manage potential threats all from one centrally managed console to ensure that all machines in the environment are protected against the ever-growing barrage of threats and malware.

Deployment is simple and took only a few minutes to get everything up and running. The initial installation required the server component be installed on a machine in the network. We found the server component to be fairly lightweight, so deployment of the server did not require a dedicated monster machine. After the server was installed, clients were deployed in a couple of different ways. The client package came as an MSI file, so we chose to deploy using Active Directory Group Policy. We found installation and deployment of the clients to be easy and straightforward.

After the server was installed and the clients deployed, all further management and configuration was done using the management console application on the server. We found this console to be simple to use and navigate, but it did take a few minutes to get acquainted with how to configure various policies to actually manage machines. With that said, this product provided a lot of great management capabilities and systems overview functions. The intuitive dashboard of the console gave a great overview of non-compliant or out-of-date systems and allowed for the push of updates with a single click of the mouse.

Documentation included both basic setup and full administrator guides. The former offered a quick overview of how to download and install the various components, along with a brief set of instructions on how to get a base policy in place and get the product up and running. The latter offered a lot more detail on both configuring the product and using features, along with many step-by-step instructions and feature descriptions. We did notice that while the basic setup guide had a lot in the way of screen shots and examples, the administrator guide lacked in this area. We would like to see more visuals throughout the administrator guide to enhance the documentation overall.

The company offers customers ongoing, no-cost, 12/5 phone- and email-based technical support. However, if 24/7 support is needed, customers can purchase a premium plan with options that start around $500 per year. Also, products are licensed on a per seat basis, and a free version is available to customers at no cost is a large web-based area that includes a sandbox which will run any malicious files and display what is going on.

As for policy configuration, during the initial deployment the installation wizard allowed for a base policy to be set. We found this to be helpful as we could build a reasonable default policy right out of the gate without having to spend a lot of time learning how to configure policy before protection was deployed. After the initial policy was set in the wizard all further policy and configuration was done via the management console. We found this console to be a little bit scattered at first and it took a few minutes to become comfortable moving around within the console and configuring the various options. One thing that caught our attention was that changes are not applied and deployed immediately. The administrator can build policy and do all configuration necessary and then roll it out at their discretion to any or all of the machines in the enterprise.

Documentation included a getting-started guide along with a full administrator manual. The getting-started guide walked the administrator through the steps of initial installation, as well as how to get the base configuration set up. After that the administrator manual was used to find more in-depth information on using the product and configuring product features and functions. Both guides included a multitude of screen shots, step-by-step instruction that were easy-to-follow, and many diagrams and configuration examples.

ESET includes the first year of support in the initial purchase prices of the software. After the first year, customers can purchase additional aid as part of an annual contract. ESET offers 24/7 phone- and email-based technical support for customers along with a full assistance area on the website.

At a price starting around $600 for 25 machines, we find this product to be a great value for the money. While there are not very many flashy extra features beyond simple port and device management, this tool comes up solid for ensuring that machines are locked down on a granular level to prevent data leaks or any of the other potential problems that go along with use of unauthorized devices in the network.

GFI EndPointSecurity 2012

GFI EndPointSecurity 2012 provides administrators a simple way to lock down computers across the enterprise network to ensure only authorized removable media devices are used to protect against data leaks and potential infection from malware. This product features easy-to-use controls to allow or deny the use of USB flash drives and other types of portable media based on already existing Active Directory users, groups or computers. Further more, granular controls can be used to manage devices by class, physical ports on the machine, device ID or even specific file types and extensions.

Installation was quite straightforward. The two-part installation process consisted of installing the server software on a machine in the network and then deploying the agent service across the network using the administration console. We found the agent deployment to be seamless and straightforward because the application identified all Active Directory computers in the network on install. It took just a few clicks and we had agents deployed on all machines. As for the server software, installation only took a couple of minutes and was aided by an easy-to-follow installation wizard.

As for policy configuration, during the initial deployment the installation wizard allowed for a base policy to be set. We found this to be helpful as we could build a reasonable default policy right out of the gate without having to spend a lot of time learning how to configure policy before protection was deployed. After the initial policy was set in the wizard all further policy and configuration was done via the management console. We found this console to be a little bit scattered at first and it took a few minutes to become comfortable moving around within the console and configuring the various options. One thing that caught our attention was that changes are not applied and deployed immediately. The administrator can build policy and do all configuration necessary and then roll it out at their discretion to any or all of the machines in the enterprise.

Documentation included a getting-started guide along with a full administrator manual. The getting-started guide walked the administrator through the steps of initial installation, as well as how to get the base configuration set up. After that the administrator manual was used to find more in-depth information on using the product and configuring product features and functions. Both guides included a multitude of screen shots, step-by-step instruction that were easy-to-follow, and many diagrams and configuration examples.

GFI includes the first year of support in the initial purchase prices of the software. After the first year, customers can purchase additional aid as part of an annual contract. GFI offers 24/7 phone- and email-based technical support for customers along with a full assistance area on the website.

At a price starting around $600 for 25 machines, we find this product to be a great value for the money. While there are not very many flashy extra features beyond simple port and device management, this tool comes up solid for ensuring that machines are locked down on a granular level to prevent data leaks or any of the other potential problems that go along with use of unauthorized devices in the network.
Identity Finder DLP Suite

The Identity Finder DLP Suite takes an interesting look at securing the endpoint. This product does not deal with locking down ports or limiting functionality to protect against data leakage, but rather looks for sensitive information on the endpoint and provides ways to deal with that sensitive information to meet compliance standards. Administrators can use this product to remotely scan and search remote machines for personal information – such as Social Security and credit card numbers, passwords, PINs and birth dates, among many others. It then can remediate possible compliance violations by shredding, redacting, encrypting or quarantining the sensitive data.

Installation of this product consisted of installing up to three components. The first installed was the server itself. We found installation to be a simple but slightly long process. We also found that the server software relied on several prerequisites that must be met exactly or the installation will not move forward. For example, this product used a backend SQL server database, but the only database support was the most recent version of Microsoft SQL Server. If there was no instance of SQL Server 2008 or later in the environment a new installation had to be done before the installation of the server would continue. After the server was up and running, the two other components were the agents for both Windows and Mac. These agents were simple to deploy throughout our environment. There was also an option to deploy agents through an Active Directory Group Policy Object.

Once installation was complete, all further management was done through a management console, which we found to be well organized and intuitive to navigate. The dashboard view within the console provided a fairly detailed overview of endpoint status and gave a good bird’s-eye view of where possible problems lay. We also found that the software relied on several prerequisites that must be met exactly or the installation will not move forward. There was also an option to deploy agents through an Active Directory Group Policy Object.

Documentation included a couple of guides and manuals. The documentation was broken up into separate documents for both the console and endpoints. The console documentation featured installation and full user guides. We found that the installation guide offered a great amount of detail on the setup process and how to get the product up and running with an initial configuration. The user guide also was detailed, but did not go into as much depth as we would have expected. With that said, we found all documentation to be well-organized and easy-to-follow. Identity Finder offers no-cost support to all customers in the form of an online knowledge base, user forum and access to online FAQs and product documentation. The user guide also was detailed, but did not go into as much depth as we would have expected. With that said, we found all documentation to be well-organized and easy-to-follow.

Identity Finder offers no-cost support to all customers in the form of an online knowledge base, user forum and access to online FAQs and product documentation. As well as eight hours a day/5 days a week phone- and email-based technical support. Customers with subscription-based licenses also get 12/5 phone- and email-based technical assistance, along with dedicated support agents and remote troubleshooting aid.

With prices ranging from $5 to $20 per seat, depending on volume and license duration, we find this product to be an excellent value for the money. This suite includes some great features for ensuring that sensitive information spread

McAfee Total Protection for Endpoint

Total Protection for Endpoint from McAfee offers just what the name says: a full-scale suite of tools to protect and secure endpoints throughout the enterprise and ensure that policy compliance is met across the board. Some features include full disk encryption, device management to control use of removable media, intrusion prevention, local firewall, email virus and spam protection, web content filtering and security, network access control, and virus and malware protection. All of this functionality can be controlled and monitored by administrators from one central console. With all of the features and functions that are packed in this product one would think it would be difficult to deploy and configure. We found that this was not the case at all. The initial implementation consisted of installing the server software on a machine in the enterprise. The installation itself was launched from an executable and, after a short setup wizard, the installation took just a few minutes to complete. The installer initiated all necessary components along with any prerequisites that were needed. So, installation was seamless without the need to start and stop to install missing prerequisites. After the server was installed, deploying agents across the network was easy and done from right within the web-based management console.

We found the management console to be easy to navigate with intuitive controls. The layout was very comfortable to browse around in and we had almost no trouble at all becoming acquainted with how to use and configure the product. This tool featured a robust policy engine that had many granular controls and options. We also found that this solution had a lot of auditing and reporting ability, making it simple to find and remediate non-compliant machines right from the comforts of the console.

Documentation provided with this product was comprised of a quick-start guide and several other product manuals for each of the various components of the suite. The quick-start guide featured a well detailed overview of both installation and post-installation tasks to get the product up and running with an initial configuration. From there the individual manuals took over for information and detailed instructions on how to configure the individual components that make up the suite. While we found all documentation to be satisfactory – with many screen shots, diagrams and step-by-step instructions – we would like to see it consolidated into one solid document for the suite. McAfee offers full 24/7 phone and email technical support as part of a subscription. Customers also get access to a vast online portal with resources, such as a knowledge base, product documentation, online chat aid and a user forum, among many other helpful components.

At a price starting at around $231 per node for up to 25 nodes, this product could become quite expensive for larger environments. However, we find it to be a very good value for the money as it features a lot of functionality bundled up into one easy-to-use and manage package. If purchased ala carte, adding many of the components would become quite pricey. However, this product gives all the functionality under one management umbrella. Overall, McAfee Total Protection for Endpoint is a solid product and a good value.
Novell Endpoint Protection Suite

The Novell Endpoint Protection Suite features two modules from the much larger ZENworks Suite of products. Making up the Endpoint Protection Suite are ZENworks Endpoint Security Management and ZENworks Full Disk Encryption. Optionally, ZENworks Patch Management can be added on for system patching and remediation capabilities. The Endpoint Security Management piece of this product features VPN enforcement, personal firewall, wireless security enforcement, USB and device and application control, along with removable storage device and file and folder encryption. Further enhancing security, Full Disk Encryption ensures that all endpoints have fully encrypted hard drives.

Installation and deployment was straightforward and did not require much effort from the administrator. The server software was installed in both Windows and Linux platforms providing deployment flexibility. We chose to do a Windows-based installation for our review and found we had the server installed and up and running in no time. After the server was installed, all further management was done via a well-organized management console. We found this to be simple to use and intuitive to navigate. After spending just a few minutes configuring policies, we were deploying agents and policies with no trouble at all.

Overall, this suite offered a lot of functionality and control over endpoints. The Endpoint Protection Suite can leverage already existing Microsoft Active Directory or Novell eDirectory structures to manage policies based on users or computers, thus offering full integration throughout the environment. Policy also showed a lot of flexibility with policy control being either granular or as broad as needed to fit the needs of specific situations or environments.

Documentation included a quick-start guide along with a full administrator guide and a few other supplemental pieces. The quick-start guide focused on an overview of the product and its features along with a few steps to getting a base configuration in place and becoming familiar with the product itself. The administrator guide focused on the ZENworks Suite as a whole with sections for managing and configuring individual components. We found all documentation to be easy-to-follow and well-organized.

The majority of support offered by Novell must be purchased as part of the maintenance fee that is included in the cost of the product. Novell offers customers two support levels that have a range of options, including 12/5 or 24/7 phone- and email-based technical assistance, along with varying response times ranging from one to four hours. Customers also can access a large support area via the website. This area includes a knowledge base, user forum, documentation downloads and many other help items.

With prices starting around $55 per seat, plus $22 per seat for maintenance, we find this solution to be a good value for the money. Overall, the Novell Endpoint Protection Suite offers a lot of features and functionality with solid granular policy controls that can integrate well into almost any environment. This suite also offers for scalability in terms of functionality, as more features from the rest of the ZENworks Suite can easily be deployed right alongside of these components and managed directly from the same administration console.

Wave Systems EMBASSY Remote Administration Server

Deploying full hardware-based encryption throughout the enterprise can be a tricky feat in many environments. This is where the EMBASSY Remote Administration Server from Wave Systems shines the brightest. Administrators can use this product to quickly and easily manage many types of both hardware- and software-based encryption throughout the enterprise. The EMBASSY Remote Administration Server can directly interface with Opal-based self-encrypting drives and SafeNet ProtectDrive, as well as Microsoft BitLocker. This provides ultimate flexibility in encryption options both on the hardware front as well as software.

This product came to us already installed on a test server, so we cannot comment much on installation itself, but we can say that the server must have a connection to the Windows domain controller and a Microsoft SQL Server backend. After installation, all administration was done through a Microsoft Management Console snap-in. We found this to be an easy and effortless way to administer the system, as it felt quite natural to system administrators working in Active Directory. Since this product interfaced directly with Active Directory, there was no need to scan the network for machines as they were already there in the directory tree and configurations were passed on with just a simple click of the mouse.

As for functionality, as we stated before, this product is pretty much focused on providing an easy way to deploy and manage hardware and software encryption across all of the endpoints in the environment. However, for those looking to step it up a bit, this tool can pair nicely with the Safend Data Protection Suite from Wave Systems. This suite adds a lot of functionality, including full security policy templates for International Bank Account Number (IBAN), payment card industry (PCI), and the Health Insurance Portability and Accountability Act (HIPAA), among many others.

Documentation included a full administrator guide for the EMBASSY Remote Administration Server. We found this to be well-organized. It also included a high amount of detail and clear configuration instructions and examples along with many screen shots and diagrams. We would have liked to have seen some installation documentation, but none was provided.

Wave Systems offers customers a single level of 24/7 phone- and email-based technical support as part of an annual software maintenance agreement. Customers also have no-cost access to an online knowledge base, but that is really the extent of the web-based assistance.

As a price starting at around $65 per seat for the lowest volume level, we find this tool to be an average value for the money. While we do appreciate its ease of use and management through the native Microsoft Management Console snap-in, nevertheless, we find that this solution lacks quite a bit in functionality at this price level. With that said, this product does serve a purpose in being able to centrally manage device encryption across the board cleanly, quickly and easily.
GROUP TEST | Endpoint security

Arkoon Network Security
StormShield v6.x

StormShield is designed to enhance endpoint security through user control, system level security, data protection and network connectivity. The components include device control, data encryption, application control, host-based intrusion prevention system (HIPS), firewall, wireless security, anti-virus/spyware, network device control and network access control (NAC). The SkyRecon-built security modules are fully integrated into a single client to ensure continuous zero-day protection and data leakage prevention without relying solely on signatures, reputation or rule updates. The installation consisted of loading the automated install package onto our test Windows 2003 server. The process took us through the software load of the server, the database setup and the console setup. The install loaded a copy of MS SQL Server 2005 Express. There was support for pointing the application to an existing MS SQL environment. The deployment and configuration process was straightforward. We were up and running in about a half hour. There were options for deploying slave servers for a fully redundant and fault-tolerant environment. We tested in a single server environment.

StormShield uses a layered combination of enforceable policies, behavior- and signature-based protections. The rule protection works much like a firewall and allows the configuration of network and application device resource rules. There are templates available to use or can create their own. The signature-based protections deliver intrusion detection system (IDS) and anti-virus-like capabilities. These are not highly configurable other than adjusting how the management console reacts to various level threats. The behavior-based protections looks much like host-based intrusion prevention. That is, they learn the profile of how applications behave and a profile is built off that behavior. The console is launched through the server application. The user interface looks similar to a Windows tool with treed navigation and information panes on the right. Admins do need to rely on the documentation to configure as there is some complexity in navigating the menus. The application control and host-based intrusion protection were done well. The encryption protection was granular and is available by user, whole disk, specific files or folders or for removable media. Control of devices, ports and network resources were all available. There were a handful of high-level reports available for server and workstation reporting. Also, there were a good amount of graphs available summarizing top five style overviews for server and agent statistics. The logs were exportable to multiple formats. One can configure end-user alerting for various policy violations, but we didn’t see any automated event alerting for the IT and security teams. The documentation is not as solid as we would have liked. Meanwhile, support is available eight hours a day/five days a week, and renewals run at 40 percent of the base price. Assistance 24/7 is available for an additional fee.

This solution has all the pieces and is well integrated. It is at the top of the pricing scale for the solutions we evaluated.

Bit9 Parity Suite V6.0.2

Parity is a policy-driven whitelisting solution for managing the applications and devices that can run on Windows computers. Parity provides the ability to track the propagation of software in an environment, generate audit trails of portable storage activity and control the software and devices used on computers, including blocking modern malware, targeted attacks, installation of unauthorized software and execution of files from unauthorized devices.

Parity Server Software installs on Windows Server 2003 Standard or later. Admins need to have IIS (Internet Information Services) and .NET installed on the server and have SQL Server on the server or remote prior to loading the application. SQL Server 2005/2005 Express and SQL Server 2005/2008 are supported. The install was wizard driven and very straightforward. We were up and running in under 15 minutes. Once installed, the server console is accessed via any web browser.

Parity uses an agent-based approach for client management. Client stations download the agent from the server. Computers aren’t imported, they are discovered once the client is loaded. Although computers aren’t discovered via Active Directory (AD), they can be mapped to Parity policies via AD policies. Once installed, admins can gather a file inventory from the endpoints. Bit9 Parity provides continuous monitoring of all software and portable storage devices running on each endpoint. It provides an in-the-cloud, software reporting service that assigns a trust rating to all software to identify computers at risk with embedded malware. As well, it provides policy-based controls that ensure only trusted software, portable storage devices and configuration changes are made to the endpoint.

The package includes application control and whitelisting, device control, file integrity monitoring, registry protection, memory protection, operating system integrity protection, trust-based software reputation and cloud-based policies. After endpoints are under Parity control, admins approve new applications or patches using the approval methods that best suit the organization’s software rollout procedures. Parity features several automatic approval methods (trusted directories, approved publishers, trusted users and enabled updaters) that make it simple to approve new software without having to do it file by file. The user interface is easy to navigate. The homepage is dashboard driven and users have a lot of flexibility in customizing the portlets. Admins can display any of the Parity summary information or even link a portlet to an outside URL for additional data. Customers have a few policy templates and can use those to customize more. Reporting was light, but again, clients can add what they want. There was one feature that we found particularly useful: a baseline drift report.

Standard support is offered between 8 a.m. and 8 p.m., Monday through Friday, and is available at 20 percent of sale price, while 24/7 support can be purchased for 25 percent of the sales price. The documentation is well done and simple to follow. Alerting is available for configured trigger events via email, the real-time dashboards and an alert banner page.

Details
Vendor: Arkoon Network Security
Price: For quantity one purchases: $15.60, including standard support is the base price. Additional protection/modules can be added that could bring the price up to $32.00 per seat.
Contact: skyrecon.com
Ratings
Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★
Support ★★★★★
Value for money ★★★★★
Overall Rating ★★★★★
Strengths: Fully integrated, full featured.
Weaknesses: Documents did not match the install process. Reporting and alerting is a bit light.
Verdict: Great layered protection architecture on the pricey side, delivers a lot of features.

Details
Vendor: Bit9
Price: Price may vary based on terms, such as volume and length of contract. Both subscription and perpetual licenses are available, averaging about $22/EP for a perpetual license for 1,000 EPs.
Contact: bit9.com
Ratings
Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
Overall Rating ★★★★★
Strengths: Drift reporting and dashboarding.
Weaknesses: Not a lot of out-of-the-box templates for policy or reports.
Verdict: A great complement to existing firewall and antivirus endpoint solutions. The drift reporting capability is worth the investment alone.
Kaspersky Endpoint Security 8


The server software load requires Microsoft Windows Server 2003 or later, Microsoft SQL Server Standard or Express 2005/2008 and Microsoft Data Access Components (MDAC) 2.8 or later. The installation was very simple: we downloaded the software, ran it on our test server and were up and running in under 15 minutes. There is a quick-start wizard to walk admins through all the initial set up and configuration, licensing and alerting/SMT settings. We had a separate download for the client side, the Endpoint Security v8.1.0.81. The client supports most Microsoft and Mac operating systems and Debian. There is also support for virtual machines. One can use the Kaspersky Security Center application to remotely install the solution on workstations and servers, set protection parameters, manage anti-malware updates, monitor security status and respond to events. Data exchange between client computers and Administration Server, as well as Administration Console connection to Administration Server, can be performed using the secure socket layer (SSL) protocol.

The management interface is provided by the Administration Console component. It is a specialized standalone snap-in that is integrated with Microsoft Management Console (MMC). The user interface is well done, clean and very simple to use. One has full Active Directory integration for importing and discovering endpoints or users can discover endpoints by IP scans. Along with anti-virus, Kaspersky has integrated application and device control and web content filtering to Kaspersky Endpoint Security 8 for Windows. It benefits from an enhanced anti-virus engine and a range of optimization technologies designed to ensure an efficient use of workstation and server resources.

Reporting, dashboarding and alerting were all exceptional. The alerting was good on both the support and end-user side. Customers even have an integrated work流程 to allow the end-user to request exceptions to policies for enabling certain application or device access. On the support side, alerting or triggers are configurable for events via email, Net Send or to launch an executable. A few key changes from the previous version include the addition of the application control, support for Windows failover clustering to support high availability configurations, and reporting and dashboarding updates.

Standard support is offered at no charge and includes phone help between 8:00 a.m. to 9:00 p.m. EST, and full access to a knowledge base and user forums. Additionally, for 12 percent of list price, users can upgrade to 24/7 phone support. Documentation is well done, detailed and easy to use.

This is a strong contender for endpoint protection and delivers a lot of protection at a good price point while being simple to deploy and manage.

Lumension Endpoint Management and Security Suite v7.1

Lumension Endpoint Management and Security Suite (LEMSS) is an application that serves as a platform for other applications that protect a network from security risks. The Lumension OpenSpace Suite, Lumension Security Center, and the Lumension Endpoint Management and Security Suite Database Server. System requirements include Windows 2003, Web Edition/SP2, Windows 2008 R2, SQL Server 2005, Express/SP3, SQL Server 2008 R2, IIS 6.0, .NET Framework 3.5, MS internet Explorer 7 and Silverlight. Microsoft Silverlight is required during the installation and when accessing the LEMSS server. If one doesn’t have an instance of SQL Server available, the software will load SQL Server 2008 R2, Express Edition. We cannot comment on the installation process as we evaluated this solution in the provider’s cloud-based environment. From the documentation, it appears to be fairly straightforward.

Once installed, the LEMSS Agent scans the endpoint for inventory and uploads the scan results to the Lumension LEMSS server. The agent also supports snapshot generation for the various Lumension LEMSS modules. By installing these agent modules, functionality can be expanded. The tool uses Windows Firewall and requires users to have file sharing and network discovery enabled so that the endpoints can be discovered by LEMSS. SSL is used for transmitting data between the LEMSS Server and LEMSS Agents.

The asset discovery capability was good and integrated with Active Directory insufficient for the endpoint to scan by IP range and import inventory lists from the asset management system. Also, there were multiple ways to get an endpoint in easily. We found the user interface a bit cumbersome to maneuver. It took some time and effort to get through the basic setup of users and policies.

Admins can add modules as needed very easily.

Weaknesses: Lot of setup; interface takes time to work through.

Verdict: Admins can identify endpoints easily and deploy a few to several layered security solutions through a single integrated platform.

Details

Vendor Lumension
Price Subscription price of 500 nodes (assuming all components licensed): $32.99/node
Contact lumension.com

Ratings

Features
Ease of use
Performance
Documentation
Support
Value for money
Overall Rating

Strengths Reporting, dashboarding and alerting. The addition of application monitoring really adds value.

Weaknesses None noted.

Verdict: A feature-rich and strong management platform that is an excellent value for the money. This one is our Best Buy.
Quarri Technologies Protect On Q v2.7

Protect On Q (POQ) from Quarri Technologies is a security software solution that empowers organizations to protect browser-delivered content from compromise. POQ enables IT professionals to deliver and enforce secure web sessions on-demand that prevent the unauthorized use and replication of confidential data while it’s in transport and use. The solution works by protecting web sessions from pre-authentication to logout, with minimal installation requirements and without leaving installed software behind on the accessing device.

The POQ hardened browser shields sensitive data from keyloggers, frame grabbers, session hijacking, cache miners and other malware, while blocking inbound attacks as well. POQ also enables organizations to enforce security policies that prevent end-users from copying, saving, printing or screen-capturing browser-delivered data, including from browser-launched processes, like Adobe Reader, Microsoft Office or ZIP files. POQ is delivered on the fly when end-users login, ensuring privacy by encrypting session data, including cache files, cookies, password and history. All session data is overwritten and deleted at the end of the session. POQ also protects against session hijacking by controlling all browser networking.

Before installation of the POQ application, Java and Tomcat (or another Java server container) must be installed and running. The Manager installs into Tomcat 6+, or other servlet engines with Java 6+. The Server installs into Tomcat 6.0 or other servlet engines with Java 6+. After Java and Tomcat are installed, the POQ server and manager installation is fairly straightforward. One downloads and copies the WAR files into the Tomcat web apps directory, restart and then access the console via a browser through the local host address. The first thing one sees in the console is the policy screen. Administrators use the policy manager to create policies and set the default protections through the security settings that control how POQ will handle/prevent malware.

POQ enables organizations to define security policies that deliver application-specific policy settings that are packaged with the binary Enforcer components. The provisioning server can be the web application server or a remote standalone server. POQ enforces security only in the protected session. No other browser instances or applications are affected. POQ integrates directly with web servers or with popular web gateway front ends. The product can be configured to either be optional: end-user clicks a link on a web page to start the protected session; or required: end-user must be running a POQ browser in order to access the web resources.

Standard eight-hours-a-day/five-days-a-week technical support is included along with all software updates during the subscription term, while 24/7 premium assistance is available for a 15 percent addition to the software subscription fee. Documentation is good and helped us through the install and configuration activities.

Sophos Endpoint Protection v10

Sophos Endpoint Protection v10 provides a single, automated console for Windows, Mac, Unix, Linux and virtual platforms to centrally manage antivirus, firewall, intrusion prevention, web protection, patch management, encryption, device management and application management. Sophos Central Management Console requires on the endpoint. POQ enables IT professionals to deliver and enforce secure web sessions on-demand that prevent the unauthorized use and replication of confidential data while it’s in transport and use. The solution works by protecting web sessions from pre-authentication to logout, with minimal installation requirements and without leaving installed software behind on the accessing device.

The POQ hardened browser shields sensitive data from keyloggers, frame grabbers, session hijacking, cache miners and other malware, while blocking inbound attacks as well. POQ also enables organizations to enforce security policies that prevent end-users from copying, saving, printing or screen-capturing browser-delivered data, including from browser-launched processes, like Adobe Reader, Microsoft Office or ZIP files. POQ is delivered on the fly when end-users login, ensuring privacy by encrypting session data, including cache files, cookies, password and history. All session data is overwritten and deleted at the end of the session. POQ also protects against session hijacking by controlling all browser networking.

Before installation of the POQ application, Java and Tomcat (or another Java server container) must be installed and running. The Manager installs into Tomcat 6+, or other servlet engines with Java 6+. The Server installs into Tomcat 6.0+ or other servlet engines with Java 6+. After Java and Tomcat are installed, the POQ server and manager installation is fairly straightforward. One downloads and copies the WAR files into the Tomcat web apps directory, restart and then access the console via a browser through the local host address. The first thing one sees in the console is the policy screen. Administrators use the policy manager to create policies and set the default protections through the security settings that control how POQ will handle/prevent malware.

POQ enables organizations to define security policies that deliver application-specific policy settings that are packaged with the binary Enforcer components. The provisioning server can be the web application server or a remote standalone server. POQ enforces security only in the protected session. No other browser instances or applications are affected. POQ integrates directly with web servers or with popular web gateway front ends. The product can be configured to either be optional: end-user clicks a link on a web page to start the protected session; or required: end-user must be running a POQ browser in order to access the web resources.

Standard eight-hours-a-day/five-days-a-week technical support is included along with all software updates during the subscription term, while 24/7 premium assistance is available for a 15 percent addition to the software subscription fee. Documentation is good and helped us through the install and configuration activities.
Symantec Endpoint Protection 12 v12.1

Symantec Endpoint Protection 12 is a client-server solution that protects laptops, desktops, Mac computers and servers in a network against malware. It combines virus protection with advanced threat protection to proactively secure computers against known and unknown threats. The tool combines traditional scanning, behavioral analysis, intrusion prevention and community intelligence into its security system.

Endpoint Protection is most commonly installed on a Windows Server class system, with a 32-bit or 64-bit processor using either the embedded database or SQL Server database. MS SQL 2000 and above are supported. The Symantec Endpoint Protection Management client is most commonly installed on Windows XP, Windows 7 32-bit or Windows 7 64-bit systems, Mac OS X 10.5 and higher and Linux systems. Our copy was installed on our Windows 2003 Server and SQL 2005 database.

The implementation is straightforward. Admins launch the installer and the deployment is fully automated and menu driven. The binaries are fairly large, around 1.5G, but the software load went pretty fast. The Symantec Endpoint Protection Manager is loaded along with the database. We had an SQL server running on our server so it deployed using that resource. The software load took about 20 minutes. Once loaded, we were able to access the user interface for configuring our protection. The console was accessed as an application from the start menu.

The user interface (UI) is dashboard driven and attractively laid out. We had protection for anti-virus, firewall, intrusion prevention, and application and device control. Policies for each of these functional areas can be set from the UI menu. Admins can add or edit the basic policies and can get very granular as to what is to be scanned. Application control was done well. It comes with basic rules sets that users can employ, customize or add to. The device control gave granular control of setting policies. The firewall comes with a number of built-in rules and was simple to configure. The firewall had a stealth mode feature to block websites from fingerprinting endpoints. Dashboard reports were great.

Leveraging, Insight and SONAR technologies, Symantec Endpoint Protection 12 blocks new and unknown threats missed by traditional signature, heuristic, behavioral and HIPS-based security solutions. We did not test catch rates or performance claims, but the documentation does state that the technology is optimized to eliminate up to 70 percent of scan overhead, reducing load on the endpoint. For virtual environments, Endpoint Protection can whitelist images and maintain a local cache of scanned files shared across VMs reducing load on the disk farm and increasing virtual instance density.

Symantec offers basic maintenance that includes telephone support between 8 a.m. and 6 p.m. with Symantec Endpoint Protection 12. Essential support is available as an upgrade and fees vary. Documentation was sufficient to get through the install process.

Trend Micro Enterprise Security for Endpoints

Trend Micro Enterprise Security for Endpoints is a centrally managed security suite for desktops, laptops and mobile devices. We were provided a download for OfficeScan 10.6, Control Manager 6 and some plugins for intrusion defense firewall and integrated data leakage prevention (DLP). Trend Micro Control Manager 6 provides central threat and DLP policy management across layers of the IT infrastructure. Trend Micro OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware and mixed threat attacks. An integrated solution, OfficeScan consists of a client program that resides at the endpoint and a server program that manages all clients. The client guards the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every client.

The requirements for the OfficeScan Server are Windows 2003 SP2 or later. However, there are a few caveats. OfficeScan requires IIS or Apache web server and Control Manager used our MS SQL instance to install its database. We had some issues getting OfficeScan and Control Manager running on the same server. Trend Micro does not recommend installing Control Manager and OfficeScan 10.6 on the same box. Instead, it was highly recommended to install them on separate machines. After several attempts, we did get both packages to load. We launched the OfficeScan web portal. Once in, we downloaded and installed the two plug-ins mentioned above.

Enterprise Security Suite for Endpoints includes multiple, purpose-built components. OfficeScan provides real-time protection against the latest viruses and trojans and web-based threats. It uses cloud-based threat intelligence and integrated optional DLP. Intrusion Defense Firewall, a plug-in for OfficeScan, provides network-level, strong endpoint protection by supplementing highly effective OfficeScan client-level security with proactive virtual patching.

The Data Protection module provides Digital Asset Control and expands the range of devices monitored by Device Control. The Data Loss Prevention plug-in for OfficeScan includes predefined policy templates, multi-channel content filtering and granular device control. All of these solutions can be integrated through the OfficeScan Manager framework, which uses a plug-in architecture to permit easy integration of components to tailor the protection capabilities to the customer’s business and security needs.

The user interface was intuitive and we had no problem adding modules, setting policies and reviewing results. Customers can find endpoints through a scan tool. Reporting was good and offered numerous standard accounts. There was a high-level dashboard summary of key client information and threats.

Standard support is included for one year in the purchase price and includes eight-hours-a-day/five-days-a-week support. Ongoing renewal is usually 40 percent of the first year’s price. Support is available 24/7 for an additional fee of $8 to $12 per user, regardless of the product. Documentation was complete and we did need to use it to deploy and configure the software.
Cyber threats are becoming more sophisticated with the blending of once-distinct types of attack into more damaging forms. These asymmetrical threats are seen as one of the top issues in the global policy and national security agendas, and an increasingly challenging policy area for governments. This is perhaps unsurprising as cyber space was never built with security in mind.

Global reliance on information and communications technologies (ICT) and cyber space for the conduct of both business and pleasure has meant that we can not simply shut down access to ICT or cyber space to address these threats. This is true not only for more open and liberal societies, like Australia or the United States. Even authoritarian nations, such as China, can no longer consider shutting down the internet and other communication channels as a means of dealing with threat. Instead, authorities must find various strategies to build the national resilience needed to maintain an open yet secure cyber space, and to strike the most appropriate balance between the protection of citizens, national security interests and democratic freedoms.

Cyber threats and windows of vulnerability evolve over time, and therefore threat assessments should not be static. Understanding the threat landscape is crucial to a nation’s security agenda, and as explained in a U.S. Department of Defense 2011 policy report to Congress: “The United States needs to understand other nations’ cyber capabilities in order to defend against them and to improve our ability to attribute any cyber attacks that may occur.”

Technical solutions can provide effective protection against many of the existing threats, but these alone cannot provide a comprehensive solution. Different players in the digital economy are best placed to provide unique, but complementing roles in mitigating the cyber threats faced by consumers, businesses and governments.

Many sectors, particularly critical infrastructure sectors, are privately owned. Instituting an effective coordination between the public and private sectors and the research community will play a pivotal role in mitigating threats. For example, secure and trusted information-sharing mechanisms will facilitate the dissemination of timely and actionable alerts, classified or sensitive information and research findings. This would enable all parties involved to produce threat assessments based on fresh and accurate information, facilitate real-time collaboration to stop malicious cyber incidents in progress, and investigate cross-border activities.

In the competitive and fast-developing landscape of cyber threats, it is essential to canvas global developments in the criminal, political, regulatory and business environments which may give rise to malicious activities, as many of the risks are based in global features of the criminal economy and the global threat landscape. This would allow us to provide current and relevant policy and practice evidence with much broader international, inter-sector and interdisciplinary perspectives. In turn, this would inform governments’ policy and operational responses to cope with the emerging cyber threat landscape in a climate of enduring fiscal restraint. In addition, integrating perspectives and approaches from different sectors, research disciplines and countries would allow governments and the general society to identify existing weaknesses in regulatory behavior, ways to design measures to address them more effectively, and ensure that the responses are harmonized with international best practices.

Raymond Choo is a senior lecturer at the University of South Australia.

“Cyber space was never built with security in mind.”
YOUR FINAL BUSINESS SECURITY DESTINATION

Buy 1 license, get 1 FREE!*  

Purchase a minimum of 25 seats of ESET Endpoint Antivirus or ESET Endpoint Security and receive an equal number of one-year ESET NOD32® Antivirus 4 Business Edition for Mac seats AT NO ADDITIONAL COST!  

Valid from 6/15/2012 through 9/30/2012.  
*Terms and conditions apply. Visit www.eset.com/q3promo-trial for details.

New ESET Endpoint Solutions solve your need for risk mitigation and uninterrupted network uptime so you can be confident in your security posture.

ESET keeps your systems running 24/7/365  
• Powerful, accurate detection  
• Low false positives  
• Data access and control  
• Proprietary ThreatSense® for detection of unknown threats

www.eset.com  
Ready to get started?  
Get your free trial today.