FEATURES:

PRIVACY MATTERS

Greater connectivity has changed the way we view privacy, says Hilary Wandall, CPO, Merck. P18

The data backlash
Is resistance forming against data-sharing? The consensus: “Yes.” P24

Passing the buck
Who pays what to cover the cost of stolen credit card information? P26
REGULARS

4 Editorial Trifecta 2.0: Trust, privacy and security.

8 Threat report A hacker claimed to have compromised data related to South Korea’s power plants.

10 Threat stats There were three million attacks in the United States last month.

12 Update Data of 11 million Blue Cross customers may be at risk.

13 Debate Congress should mandate the payment card industry adopt safer technology.

14 Two minutes on… Solutions going to waste.

15 Skills in demand Information security recruiters are needed.

17 Opinion IT only guards the front gate, by Lena Smart, CIO, New York Power Authority.

18 Privacy matters Greater connectivity has changed the way we view privacy – and the Fourth Amendment, says Hilary Wandall, CPO, Merck.

24 The data backlash Is resistance forming against data-sharing in America? The consensus seems to be a resounding “yes.”

26 Passing the buck The battle over who pays what to cover the cost of stolen credit card information is heating up.

28 Sign on the digital line Biopharma companies need a secure digital signing infrastructure. SureClinical found an answer for them.

31 Product section The theme this month is SIEMs and UTMs and where they fit into your enterprise.

32 Group Test: SIEM and UTM SIEMs take in data from multiple sources, normalize it and correlate it so that conclusions can be drawn and decisions made. UTM tools offer several advantages over point solutions. You likely need both.

YOUR FATE WILL BE DETERMINED BY YOUR SPEED OF DETECTION AND RESPONSE.

That’s where we come in. LogRhythm’s next-generation security intelligence platform identifies high-impact threats and neutralizes them before they can result in a material breach. It uniquely unifies SIEM and log management with network and endpoint forensics and advanced security analytics to provide comprehensive threat life cycle management and the ideal foundation for today’s cyber security operations.

IMPROVE YOUR SECURITY INTELLIGENCE POSTURE AT LOGRHYTHM.COM/SIMM

Check Point P14

Asaf Cidon P17

Dell SonicWALL P38

Hilary Wandall, CPO, Merck P18

PRODUCT REVIEWS

31 Product section

The theme this month is SIEMs and UTMs and where they fit into your enterprise.

32 Group Test: SIEM and UTM SIEMs take in data from multiple sources, normalize it and correlate it so that conclusions can be drawn and decisions made. UTM tools offer several advantages over point solutions. You likely need both.
Editorial

Trifecta 2.0: Trust, privacy and security

To trust is to put your faith in someone’s honesty and integrity. The decision to trust typically is based on a general expectation that someone’s ethics and principles, possibly along with what they stand for and the genuineness of their actions, reflect your own.

It’s a big ‘ole gift to give – trust. And, as such, the recipient should handle it with some care and maybe a bit of reverence. Among all the critical components and thoughts and feelings on which many of our most rewarding and satisfying relationships are based, trust ranks quite high.

This is true not only of our personal associations, but also of our business partnerships, whether within our own companies or with those that we have with other organizations.

And for quite a few of these bonds, trust directly correlates to our expectations of the privacy and security surrounding the interchanges we have as part of them.

In fact, for a lot of us, trust, privacy and security are top of mind when it comes to our dealings with people, private companies, government entities and other organizations.

The problem is, as we pursue both this edition’s cover story by Associate Editor Teri Robinson and a supporting feature by Editorial Assistant Ashley Carman, these aspects of the relationships we have with businesses and our government have been compromised to such a degree that most of us are feeling huge losses – including not only a demise of trust, privacy and security, but of control as well.

According to the experts quoted in our cover story, on top of private citizens’ worries, security and privacy officers within companies have their own share of trepidations, including such things as dealing with government requests for information about customers/clients or more, the legal ramifications of moving data across borders or how they meet privacy requirements noted in European Safe Harbor laws.

The problem of maintaining trust, privacy and security is extremely complex, but as this edition’s features showcase, it is one that must be mulled and tackled with the greatest of aplomb and deference. Failing to do so, could vastly reshape the intense demands on companies and already is resulting in a search and the embrace of technologies and services that allow for citizens to wrench back some control over how they dole out trust and just what information they keep private.

Meantime, we welcome to SC’s bullpen Robert Abel, our new online coordinator, who will help in the continued development of our online presence, and we say a sad goodbye to our long-standing Online Editor Marcos Colón, whose replacement will be announced shortly. We wish both these gents only the best in their future endeavors.

Ilenna Armstrong is VP, editorial of SC Magazine.

© 2015 Raytheon Company. All rights reserved.
“Customer Success Is Our Mission” is a registered trademark of Raytheon Company.
Welcome Center Welcome Center is a portal that allows IT security professionals to register for multiple events at the same time. This new portal offers all of our U.S.-based online events and will soon include our U.K.-based ones as well. Please visit us today for all the latest insights in cybersecurity.

Maybe you’ve heard of it already. But did you know that SC Magazine has just launched a Welcome Center for our online events? This new portal allows you to:

• Register for multiple events all at the same time;
• See all our offerings in a few clicks and attend from your desktop; and
• Earn CPE credits for doing so.

Visit us at http://engage.eventb.co.rt/scwc
Russia top producer of zombie IP addresses
For the period reported, the EMEA region (Europe, Middle East, Africa) was the leading source of all zombie IP addresses. Of the countries making up the EMEA, Russia was the top producing country. For the other regions, the top producers were Argentina in South America, the United States in North America and Vietnam in the Asia-Pacific region. (Source: Symantec)
There were three million attacks in the United States last month.

Top 10 names used by phishing websites

1. Facebook 5,488,281
2. mail.com 4,385,648
3. MAIL.RU 3,441,688
4. Google 3,340,121
5. LinkedIn 2,472,579
6. CNBC 1,820,369
7. Microsoft 1,075,126
8. Telstra 1,052,018
9. EarthLink 890,533
10. groupon 821,809

Top 5 attacks used by U.S. hackers

1. Upatre Downloader trojan
2. CryptoWall trojan
3. Waledac trojan
4. Gozi trojan
5. Downloader trojan

Top 5 attacks used by foreign hackers

1. ZeroAccess trojan
2. Butterfly botnet
3. Gozi trojan
4. Dyre banking trojan
5. Downloader trojan

Top 5 sources of spam

- United States 19.86%
- China 9.53%
- Vietnam 4.99%
- Ukraine 4.64%
- Russian Federation 4.30%

Top 5 attacked countries

- Croatia 2.75%
- Algeria 1.54%
- Russian Federation 1.28%
- Tunisia 1.27%
- Kazakhstan 1.25%

Top breaches in March

- Advantage Dental: 151,626 records
- Redmond, Wash.: Advantage Dental notified patients of a data breach when its database of patient information was hacked between February 23 and February 26. The hackers had access to patient names, dates of birth, phone numbers, Social Security numbers and home addresses.

TOTAL number of records containing sensitive personal information involved in breaches in the U.S. since January 2005: 816,324,756 (as of April 13)

Index of cybersecurity

- Perceived risk: 6.5
- Index value: 2.650

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

Source: ICS, www.cybersecurityindex.com

Internet dangers

- Top 10 threats
  1. Upatre.aa 05/09/14 downloader 0 0
  2. Upatre 12/11/13 downloader 0 0
  3. Simbot.gen 06/29/11 backdoor 0 0
  4. Soltern.i 03/08/11 worm 13 7
  5. Tugsay.a 07/07/14 downloader 3 2
  6. Ogmarkgen 09/17/14 downloader 0 0
  7. Eggnog.a 01/15/14 worm 0 0
  8. Berbew 01/31/11 backdoor 0 0
  9. Ramnit.i 12/03/10 virus 11 1
  10. Ramnit.a 01/05/11 virus 0 0

Source: Motive Security Labs

Zombie IP addresses are recorded in CYREN’s database as having sent spam in the past 24 hours. These are infected computers (zombies) that are unknowingly sending spam. Based on the IP address, the company can determine the country of the spam-zombie and then sums up the spam-zombies per country.

Source: Dell SecureWorks

Source: CYREN

Top 10 names used by phishing websites

- Facebook: 5,488,281
- mail.com: 4,385,648
- MAIL.RU: 3,441,688
- Google: 3,340,121
- LinkedIn: 2,472,579
- CNBC: 1,820,369
- Microsoft: 1,075,126
- Telstra: 1,052,018
- EarthLink: 890,533
- groupon: 821,809

Source: Kaspersky

Source: Privacy Rights Clearinghouse (data from a service provided by DataLossDB.org, hosted by the Open Security Foundation)
President Obama issued an executive order with the aim of combating “malicious cyber-enabled activities” executed wholly, or in “substantial part,” by foreign attackers targeting the U.S. The executive order detailed a new sanctions program which authorized the Secretary of the Treasury, in consultation with the Attorney General and Secretary of State, to sanction threat actors posing a significant threat to the nation’s safety or economy. Obama, who declared the threat a national emergency, said the sanctions would apply to individuals who harmed or significantly compromised a computer (or network of computers) that support one or more entities in the critical infrastructure sector. Foreign attackers that cause a “significant misappropriation” of funds or economic resources, financial data, trade secrets or personal identifiers are also among those who could be blocked from all financial dealings with the U.S.

The personal data, including bank account information, of 11 million Blue Cross customers may have been compromised.

The retail space has been hit hard, with the personal information of millions of customers compromised. The simple fact is, the lack of a strong credit card authentication infrastructure has made it easier for big-box retailers – specifically Home Depot and Target – to get breached. However, the U.S. faces resistance with American retailers because they have to foot the bill for chip- and PIN systems. Despite the U.S. typically being at the technology forefront, it is more than a decade behind many other countries in adopting this system. Meanwhile, chip-and-PIN is the standard in much of Europe and other developed countries around the world. Congress mandates requiring organizations to adopt chip-and-PIN will solve what should have been solved five years ago – preventing hackers from breaking into retailers and installing malicious software on magnetic-stripe cards. We’ve seen point-of-sale systems being hit hard for years. It’s high time Congress step in to help put a stop to this.

Prognosis: Negative
Premera Blue Cross confirmed that information belonging to roughly 11 million members and applicants may have been compromised after an unauthorized intruder accessed its IT systems. That initial attack took place on May 5, 2014, but the company learned of the incident on Jan. 29 of this year. Data that was potentially accessed in the breach varies, as Premera holds different types of data on individuals.

“[CISA] is only acceptable if there are strong protections for the privacy rights of law-abiding American citizens.”

– Sen. Ron Wyden (D-Ore.), the only member of the Senate Intelligence Committee to vote against the bill.

The personal data, including bank account information, of 11 million Blue Cross customers may have been compromised.

President Obama issued an executive order with the aim of combating malicious cyber-enabled activities” executed wholly, or in “substantial part,” by foreign attackers targeting the U.S. The executive order detailed a new sanctions program which authorized the Secretary of the Treasury, in consultation with the Attorney General and Secretary of State, to sanction threat actors posing a significant threat to the nation’s safety or economy. Obama, who declared the threat a national emergency, said the sanctions would apply to individuals who harmed or significantly compromised a computer (or network of computers) that support one or more entities in the critical infrastructure sector. Foreign attackers that cause a “significant misappropriation” of funds or economic resources, financial data, trade secrets or personal identifiers are also among those who could be blocked from all financial dealings with the U.S.

The personal data, including bank account information, of 11 million Blue Cross customers may have been compromised.

The retail space has been hit hard, with the personal information of millions of customers compromised. The simple fact is, the lack of a strong credit card authentication infrastructure has made it easier for big-box retailers – specifically Home Depot and Target – to get breached. However, the U.S. faces resistance with American retailers because they have to foot the bill for chip- and PIN systems. Despite the U.S. typically being at the technology forefront, it is more than a decade behind many other countries in adopting this system. Meanwhile, chip-and-PIN is the standard in much of Europe and other developed countries around the world. Congress mandates requiring organizations to adopt chip-and-PIN will solve what should have been solved five years ago – preventing hackers from breaking into retailers and installing malicious software on magnetic-stripe cards. We’ve seen point-of-sale systems being hit hard for years. It’s high time Congress step in to help put a stop to this.

Prognosis: Negative
Premera Blue Cross confirmed that information belonging to roughly 11 million members and applicants may have been compromised after an unauthorized intruder accessed its IT systems. That initial attack took place on May 5, 2014, but the company learned of the incident on Jan. 29 of this year. Data that was potentially accessed in the breach varies, as Premera holds different types of data on individuals.

“[CISA] is only acceptable if there are strong protections for the privacy rights of law-abiding American citizens.”

– Sen. Ron Wyden (D-Ore.), the only member of the Senate Intelligence Committee to vote against the bill.
Studies, the cost that cyber-security solutions, and rightly millions of dollars on security solutions that are neither deployed nor used. Security solutions that are commonly referred to as shelfware, leads to what industry professionals refer to as a shelfware issue, by being as transparent as possible concerning the technology these companies buy into.

“A lot of vendors have good products and solutions, but they might oversell the concept so that it’s scalable or that the technology has high interoperability,” Ponemon says. “When you put it all together, a lot of those assertions aren’t necessarily true.”

Larry Ponemon, founder and chairman of the Ponemon Institute, agrees with the concept of clear collaboration within the enterprise, especially when IT security teams are used to operating in “isolation,” which ultimately could increase the possibility of shelfware.

However, while organizations need to make sound decisions on purchasing new solutions based on their resources, Ponemon suggests that vendors could also help address the shelfware issue by being as transparent as possible concerning the technology these companies buy into.

“What do you think of the idea of actually working as a conscious person, and IT security teams are used to dealing with the threat of modern malware introduced by bad hearted people who want to do the right thing. However, the health care sector just doesn’t have the resources to properly secure systems, networks and data as it should. The confidentiality of my family’s private health information and the threat to medical identity theft is something that keeps me pushing on.”

Of what are you most proud?

What tops the list these days is leading a great team of security professionals charged with improving the security of electronic health records in the state of Indiana. Serving as Indiana’s Regional Extension Center we have helped thousands of doctor’s better secure their patient’s data.

For what would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

What features of your current role do you most enjoy?

What features of your current role do you most enjoy?

I enjoy meeting with people who share a common interest in cybersecurity.

What was one of your biggest accomplishments?

One of my biggest challenges was having to investigate a fellow security engineer on my team who violated the trust of the organization.

What keeps you up at night?

These days it is a combination of things. As a security consultant I am privileged to work with a lot of good-hearted people who want to do the right thing. However, the health care sector just doesn’t have the resources to properly secure systems, networks and data as it should. The confidentiality of my family’s private health information and the threat to medical identity theft is something that keeps me pushing on.

What would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

For what would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

What was one of your biggest accomplishments?

One of my biggest challenges was having to investigate a fellow security engineer on my team who violated the trust of the organization.

What keeps you up at night?

These days it is a combination of things. As a security consultant I am privileged to work with a lot of good-hearted people who want to do the right thing. However, the health care sector just doesn’t have the resources to properly secure systems, networks and data as it should. The confidentiality of my family’s private health information and the threat to medical identity theft is something that keeps me pushing on.

What would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

For what would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

What was one of your biggest accomplishments?

One of my biggest challenges was having to investigate a fellow security engineer on my team who violated the trust of the organization.

What keeps you up at night?

These days it is a combination of things. As a security consultant I am privileged to work with a lot of good-hearted people who want to do the right thing. However, the health care sector just doesn’t have the resources to properly secure systems, networks and data as it should. The confidentiality of my family’s private health information and the threat to medical identity theft is something that keeps me pushing on.

What would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

For what would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

What was one of your biggest accomplishments?

One of my biggest challenges was having to investigate a fellow security engineer on my team who violated the trust of the organization.

What keeps you up at night?

These days it is a combination of things. As a security consultant I am privileged to work with a lot of good-hearted people who want to do the right thing. However, the health care sector just doesn’t have the resources to properly secure systems, networks and data as it should. The confidentiality of my family’s private health information and the threat to medical identity theft is something that keeps me pushing on.

What would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

For what would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

What was one of your biggest accomplishments?

One of my biggest challenges was having to investigate a fellow security engineer on my team who violated the trust of the organization.

What keeps you up at night?

These days it is a combination of things. As a security consultant I am privileged to work with a lot of good-hearted people who want to do the right thing. However, the health care sector just doesn’t have the resources to properly secure systems, networks and data as it should. The confidentiality of my family’s private health information and the threat to medical identity theft is something that keeps me pushing on.

What would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

For what would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

What was one of your biggest accomplishments?

One of my biggest challenges was having to investigate a fellow security engineer on my team who violated the trust of the organization.

What keeps you up at night?

These days it is a combination of things. As a security consultant I am privileged to work with a lot of good-hearted people who want to do the right thing. However, the health care sector just doesn’t have the resources to properly secure systems, networks and data as it should. The confidentiality of my family’s private health information and the threat to medical identity theft is something that keeps me pushing on.

What would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

For what would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

What was one of your biggest accomplishments?

One of my biggest challenges was having to investigate a fellow security engineer on my team who violated the trust of the organization.

What keeps you up at night?

These days it is a combination of things. As a security consultant I am privileged to work with a lot of good-hearted people who want to do the right thing. However, the health care sector just doesn’t have the resources to properly secure systems, networks and data as it should. The confidentiality of my family’s private health information and the threat to medical identity theft is something that keeps me pushing on.

What would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.

For what would you use a magic IT security wand?

I would solve the information sharing trust issues so that organizations could start to collaborate with each other to share threat intelligence.
Saying safe in cyber land

How can you stay safe in cyber land? Simple – don’t use the internet for anything...ever again! OK, maybe not so simple or feasible. But take a look at these numbers: It’s estimated that by 2018 there will be 3.6 billion internet users. That means 48 percent of the world’s population could be online and primed to be cybercrime victims.

Cybercrime is nothing if not a growth industry. According to the Institute of Electrical and Electronics Engineers (IEEE), losses in the United States in 2013 alone totaled $313 billion. Internet-based crime has risen, on average, 78 percent a year since 2010. The attacks are becoming more sophisticated – with ransomware and spear-phishing the favored approaches for cybercriminals.

It is very important for everybody at the New York Power Authority, where I am the CIO, to stay vigilant when online. We ensure that all employees and contractors receive regular online and instructor-led training. We have posters, pens, mouse pads and other cybersecurity reminders at our facilities and corporate office. We also have tags at the bottom of external emails, reminding people not to click on a link if they don’t know the sender.

One of the awareness-training courses I run is called “Staying Safe in Cyber Land.” It’s a general internet safety course that I tailor for when it’s given. For example, in March we had a short video showing the results of the “phishing email” that promised a large tax refund from the IRS. We also run in-house targeted phishing and vishing (phone-based) campaigns and then provide remedial one-on-one training to anyone who gives up their password to the “social engineer.” Those are the kinds of mistakes that can’t be made twice. The next time, it might not be my Cyber Security Team on the other end of the phone.

Speaking of passwords, I always tell people to pay attention to them by suggesting they use a meaningful phrase, rather than some boring combination of letters and numbers. We also encourage membership in the FBI Infragard. I am the energy sector chief for New York and really enjoy working with the FBI and Infragard members. There is a real feeling of camaraderie and the information sharing is always beneficial.

I believe that helping our employees keep their home networks safe is also essential. Many people access our business network from their home PC, and our anti-virus software license agreement allows us to add home PCs as part of the overall coverage. Our users are encouraged to download the application when they login from home, using our two-factor authentication portal.

I constantly remind people that cybersecurity is everyone’s business – not just the responsibility of the information technology group. They need to remember we are all in this together.

Lena Smart
CIO, New York Power Authority

Opinion

IT only guards the front gate

When an IT administrator feels that control is lost, her reaction shouldn’t be to lock down the network. When the network is locked down, employees will find a way around it to be productive. That’s why bring your own device policies that are flexible enough to acknowledge employees’ changing preferences are a step in the right direction.

To properly address threats, sensitive data needs to be encrypted at the file-level so that access can be customized and audited in real-time. Features that help prevent threats or detect and stem attacks that may be underway – like full audit trails, file-level encryption, remote device wipe and user block – are also essential.

Thanks to the cloud, file-level encryption is easier than ever to deploy and further innovation has allowed employees to avoid that telltale tradeoff between security and usability, which means companies are running out of excuses for not implementing proper data security measures. It’s time to embrace encryption, or risk your company’s most valuable asset: its data.

Araz Cidon
CEO and co-founder, Sookasa

To thine own self be true

Anthem’s refusal to allow a federal audit may not have a positive effect.

T
he “Global Megatrends in Cybersecurity 2015” survey recently released by the Ponemon Institute found that the elephant is still very much in the room. Not unsurprisingly, the research showed that senior business leadership and boards of directors are interested in what their CISOs have to say.

Often, those in the corner offices don’t see the value of information security because breaches don’t hurt the company’s profitability, executives don’t lose their jobs and they don’t go to jail – the three things that seem to top their list of concerns. To convince the boardrooms of the importance of information security, a company will have to go under, and a C-level executive will have to lose their job or go to jail as the result of a breach.

But what about Anthem? I have doubts that the Anthem breach will move the bar any further than have any of the other mega breaches which have occurred over the past five years.

The only way that a breach makes that shift is with significant personal health information (PHI) disclosures, which at this time, do not appear to have happened. If the Department of Justice opens an investigation and moves toward prosecution, that would be a game changer. I do not believe this course of action is likely. That said, Anthem’s refusal to allow a federal audit may not have a positive effect.

My point is to foster discussion among information security professionals and business leaders. Some business executives may believe that CISOs are only there to be fired when a breach occurs. Many business executives have calculated the risk and believe the bottom line impact of an information security breach is negligible to them and their company. The consumers and investors don’t care, why should the board and business executives? Who will change that perception? The CISOs, the regulators or the legislators? Time will tell.

CISO at a large health care organization
Since the fall of 2001, when Congress hastily passed the USA PATRIOT Act, and particularly after Edward Snowden lifted the veil on the extent of the National Security Agency’s PRISM program (which exposed massive government surveillance of American citizens), privacy has become a much-talked-about moving target, difficult to define and even more difficult to protect for those in private industry and government charged with its care.

“The interesting thing is how things have changed in the last two years,” says Hilary Wandall, chief privacy officer (CPO) at pharmaceutical company Merck, who notes her business “doesn’t have the same obligation under the Constitution” as companies like Microsoft or Google.

Wandall, who has served in a privacy capacity for 15 years, says that early on, privacy was driven by regulatory compliance, which became more sharply defined as the Health Insurance Portability and Accountability Act (HIPAA) was refined. But now, Merck, like other multinationals, must contend with a host of privacy issues, such as “how to move data across borders” and comply with European Safe Harbor laws, Wandall says.

“We’re very concerned about how to legally move data overseas, trying to globalize databases.”

That is particularly important because Merck, like all pharmaceutical companies, must have a mechanism for doctors and patients to report adverse reactions to drugs. And that information needs to be collected and shared without revealing certain private details.

In addition to intrusive government requests and stricter policies overseas, privacy is a puzzle that has become more complicated as an avalanche of data – generated by everything from corporate servers to wearable devices – gain both mass and momentum.

There is a certain opaqueness to the way that information is shared as well, in part because people, companies and organizations are more interconnected through technology than ever before.
When data leaves a computer or personal device, its path is not straightforward and linear. Rather, a web of interconnectedness among people, companies and machines means information is shared seamlessly (most of the time) among entities, with the implicit, if not explicit, permission of consumers and businesses that want – and have become accustomed to – the benefits of that fluid information flow. And, it is fair to expect that data volume and the speed at which it travels will pick up as the Internet of Things (IoT) comes to bear.

While information flows behind the scenes, the individualized user experience has spurned so many definitions and concepts of privacy as there are inhabitants of the planet. Technology may be the great equalizer, but it doesn’t bridge the privacy divide between generations or cultures. But if digitization has grown seemingly faster than the speed of light, our legal system has not. Digitization and tech advances have outpaced our ability to keep up. Digitization and tech advances have outpaced our ability to keep up.

The Supreme Court: Cell phone justice

“The number one challenge to privacy is the wantonness of [stealing] personal data being carried out by the millions by cybercriminals,” says Larry Clinton, president of the Internet Security Alliance (ISA), contending that the constant stream of attacks is a more serious issue than the NSA’s surveillance activities. “While privacy advocates might disagree about where to put the emphasis, security threats and privacy issues share a symbiotic relationship. The security breaches that started happening in the 21st century, “changed the paradigm for companies managing data,” says Merck’s Wandall, especially in the last few years where “much greater connectivity, devices like wearables, and variables and all of these apps” emerged and created “a complex ecosystem.” All that has changed the way we view privacy, she explains.

If digitization is the hive, then the rest of society are the proverbial hives, moving so slow it might take time-lapse photography to detect progress.

“A first grader can easily access things from all over the world,” says Clinton, noting that the lure of easy information flow “is so seductive that we haven’t thought through how to manage the downside.”

But, he says, “We are so busy eating this delicious dessert that we’re unhealthy.”

J. Trevor Hughes, CEO, IAPP

Professionals, concur. “Technology advances are exceeding our ability to manage,” he says. “There is an unprecedented gap between our ability to develop standards and the bleeding-edge of technology. With the rise of social media, he adds, “we don’t know what the social norm is.”

The private sector, government and consumers have all benefited from the ease at which information flows, but are just starting to see consequences. “People expect everything to be connected, but at some point don’t recognize that hundreds of organizations are in their ecosystems,” says Wandall. “They don’t necessarily want to understand the complexity and they don’t understand the risk.” That is, until something happens. “Then they begin to realize that this is a very complex world and bad things can happen,” she says.

IBM has said that 2.5 exabytes of data was produced each day in 2012, while the BBC reported that 75 percent of it was unstructured. That is a lot of data.

“All the digital footprints we’re leaving tell a story,” says Malcolm Harrys, vice president of the Internet Security Group and chief security and privacy officer (CSPO) at Intel. And adds Matt Prewitt, partner, chairman of cybersecurity and data privacy practice, Schiff Hardin, “There is a problem of information online that vastly exceeds capability of law enforcement to handle.”

And it’s only going to grow and move faster and leave more digital trails in light of the emerging Internet of Things (IoT) when products – be it refrigerators, toasters and cars – all contribute their “voices” to the chorus of data on the internet, leaving companies grappling with how to respect consumer privacy. “How do you know where data is?” asks Wandall. “What are people’s expectations of how we use data?” Wandall says consumers authorize the initial use of their data, but “they don’t expect the secondary and tertiary uses.”

Intelli’s Harrys points to a Harris poll in which “we found 60-65 percent have no idea who has access to their data and a little over half wouldn’t be able to show if it was to society’s benefit.”

That struggle is reflected in the law itself. New data and recommendations is “something not addressed very well with current legislation,” says Wandall.

What’s behind you?

Don’t look back, but you’re being followed by the law. While those words are rarely comforting, they’re doubly insidious when it comes to privacy, applying both to law enforcement’s questionable tracking practices and to privacy legislation itself, which has seriously lagged behind the great leaps in data generation and flow that tech advances have wrought.

“The number one challenge to privacy is the wantonness of [stealing] personal data being carried out by the millions by cybercriminals,” says Larry Clinton, president of the Internet Security Alliance (ISA), contending that the constant stream of attacks is a more serious issue than the NSA’s surveillance activities. “While privacy advocates might disagree about where to put the emphasis, security threats and privacy issues share a symbiotic relationship. The security breaches that started happening in the 21st century, “changed the paradigm for companies managing data,” says Merck’s

J. Trevor Hughes, CEO, IAPP

How do we know where data is?

– Hilary Wandall, CPO, Merck

The ECPA is hardly the only privacy-related legislation (or law for its time) that was the subject of an express House resolution. It was, as its title would suggest, “a resounding loophole regarding access to stored email in the interest of public safety,” as says Wessler, but the House can’t get it to the floor for a vote. Last year’s revival and this year’s stall have been described as “a disappointment to privacy advocates and industry that are seeking serious privacy guidelines.

The ECPA is hardly the only privacy-related legislation (or law for its time) that was the subject of an express House resolution. It was, as its title would suggest, “a resounding loophole regarding access to stored email in the interest of public safety,” as says Wessler, but the House can’t get it to the floor for a vote. Last year’s revival and this year’s stall have been described as “a disappointment to privacy advocates and industry that are seeking serious privacy guidelines. The ECPA is hardly the only privacy-related legislation (or law for its time) that was the subject of an express House resolution. It was, as its title would suggest, “a resounding loophole regarding access to stored email in the interest of public safety,” as says Wessler, but the House can’t get it to the floor for a vote. Last year’s revival and this year’s stall have been described as “a disappointment to privacy advocates and industry that are seeking serious privacy guidelines.
Fourth Amendment

We’re certainly concerned from the government standpoint."

– Nuala O’Connor, Center for Democracy & Technology

And what might get Congress to move and bring them up to speed on today’s technological realities? “They’re going to have to have a Bork moment,” says Wilson, referring to former President Ronald Reagan’s failed Supreme Court nominee, Robert Bork, whose video rental history leaked during his confirmation hearings, spurring the creation of the Video Privacy Protection Act of 1988. “Then they’ll have more desire to be educated—once information about a high-level person is leaked or gets stolen or accessed.”

Or maybe Congress simply needs a nudge from the executive branch, which lately has come in the form of Executive Orders and presidential declarations meant to move legislation forward that protects data and the privacy of U.S. citizens. In a flurry of pen strokes, Obama has called for national security declarations meant to have to have a Bork moment,” says Halpert, partner, DLA Piper. He cautions that Congress get legislation right is still a stand against these requests. And, although Wandall notes that Merck doesn’t hold the kind of data typically requested by government, it has to share information on adverse drug reactions and under fair employment requirements. The company realizes, too, that it could run into Fourth Amendment issues if, say, “employees are surveilled,” he says.

“Spooks have been spying on each other forever,” says ISAs Clinton. “Digitalization created more opportunities that [the NSA community] had never had before and the tendency was to use it.”

The bigger shock came from the revelation that the government had been collecting data on its own citizens. Also, Snowden’s revelations not only showed the extent to which the government has been putting pressure on private sector companies—like AT&T, Microsoft and Google—to produce information, often without warrants, on its customers, but also, some hinted at how readily corporate America has shared information in the past with government, where it could hurt business.

Whether to have the economic incentives or an ethical commitment to privacy protection, or both, companies are beginning to publicly fight back and take a stand against these requests.

Microsoft is currently locked in a court battle over the U.S. government’s efforts to obtain customer email stored on a server in Ireland—a after the government tried and failed to access the content of emails on a server in Dublin. The non-content data was stored in the U.S. Microsoft refused and in the process has challenged court findings and been held in contempt of court, but it has also drawn support from privacy organizations and business rivals. The Electronic Frontier Foundation (EFF) filed a brief contending that capitulation would constitute “Fourth Amendment seizure,” with the user losing “the ability to decide who gets the messages and for what purposes.”

What to do?

Given the vastness of data collected, the interconnectedness in society and the legs in laws, are the Fourth Amendment and other privacy conundrums even solvable? “We’re not stating to be able to cure the disease,” says ISAs Clinton. “What we’re really trying to do is build an immune system for ourselves.”

The antibodies that will strengthen corporate privacy must come from all quarters—legislative, regulatory, judiciary, technological and corporate initiatives, and largely the consumers themselves. The path to remediation must include “a comprehensive program to harden infrastructure,” he says.

Progress likely depends, foremost, on a shift in history. Companies, even those without constitutional obligations, must begin to view themselves as “two companies. Almost every company is becoming a tech company or has a reliance on it,” says Harkins.

As proof, he points to a cement company that is putting sensors in cement so that they can be used to gather information on traffic, infrastructure erosion and the like. And, although Wandall notes that Merck doesn’t hold the kind of data typically requested by government, it has to share information on adverse drug reactions and under fair employment requirements. The company realizes, too, that it could run into Fourth Amendment issues if, say, “employees are surveilled,” he says.

“We’re certainly concerned from the government standpoint,” says Nuala O’Connor, executive director of the Center for Democracy & Technology, who notes that “the threat of terrorism is real, but you just can’t go around surveilling everything.”

But, lately privacy concerns have drawn the Fourth Amendment out of seclusion and into a very public discussion. The ACLU’s Wessner wrote recently in a blog that documents (after much stalling) under Florida’s Sunshine Laws about Stingray use there, “paint a detailed picture of police using an invasive technology more than can follow you inside your house—in many hundreds of cases and almost entirely in secret.”

That law enforcement and government too a difficult line between ensuring public safety and protecting privacy, sometimes crossing over it, is nothing new. But technology extends their reach and makes access and gathering large volumes easier. “Spoons have been spying on each other forever,” says ISAs Clinton.

“Digitalization created more opportunities that [the NSA community] had never had before and the tendency was to use it.”

The bigger shock came from the revelation that the government had been collecting data on its own citizens. Also, Snowden’s revelations not only showed the extent to which the government has been putting pressure on private sector companies—like AT&T, Microsoft and Google—to produce information, often without warrants, on its customers, but also, some hinted at how readily corporate America has shared information in the past with government, where it could hurt business.

Whether to have the economic incentives or an ethical commitment to privacy protection, or both, companies are beginning to publicly fight back and take a stand against these requests. And, although Wandall notes that Merck doesn’t hold the kind of data typically requested by government, it has to share information on adverse drug reactions and under fair employment requirements. The company realizes, too, that it could run into Fourth Amendment issues if, say, “employees are surveilled,” he says.

“The best way to implement privacy is by design,” and that’s how Microsoft has built its privacy organization. “In 1972 there were less than 200 strong. Lynch says privacy at the company includes a set of policies and procedures. “We have privacy officers embedded and ensure as we implement new products and procedures that we keep up with standards,” he says.

It would behoove companies, too, for security and privacy teams to work together more closely. Security, a more IT-oriented discipline, “can be tone-deaf to privacy,” says Harkins. “Security and privacy need to think of themselves more as magnetic bonds” that create a stronger force when they work together. Microsoft also advocates “transparen- cy, control and security around the gathering and use of data.”

Merck, says Wandall, also tries to be transparent by providing comprehen- sive privacy notices to its stakeholders, explaining information it shares. Similarly, companies like Google and AT&T are addressing the Fourth Amendment quandary, releasing transparency reports that list government requests for data—which are significant. A Facebook report shows that requests from global governments increased by around 24 percent in the first half of 2014 over the last half of 2013.

While the reports offer some insight, the U.S. government, which only recently began allowing companies to more concretely report these numbers, still provides restrictions on how much they are allowed to share. Still, baby steps are better that no steps forward at all.

But private industry needs the help of legislators, who must move quickly and decisively. Passing an information-sharing bill should be a no-brainer. “Sophisticated players are sharing info already— it’s a good practice,” says Jim Halpert, partner, DBA Piper. He cautions lawmakers not to create legislation that will make that process more complicated, but says, “Overall, though, as the legislative process moves forward it is likely to meet middle ground that works.”

In fact, he predicts, “if there’s one thing that’s going to get done, it is going to be this,” despite privacy hold-ups over fears that government might use information shared in some other context.

Likewise, the much-maligned CPBR might gain traction if interested parties take the first draft as a first step. “With additional work, it could be useful,” says Wandall. “It’s cross-sectoral [and] having legislation being considered that is cross-sectoral is beneficial.”

But, Wandall believes that the CPBR might have a more difficult time getting a thumbs up from Congress. “I’m not convinced it’s going to move,” she says.

Here comes the judge

It is more than a little ironic that the Supreme Court, upon whose bench sits a panel of jurists whose average age hovers around 70, has made some decidedly modern rulings that expand privacy protections (see sidebar, page 20). Though, in all fairness, the Supreme Court has taken its time in this career as lawmakers, says Wilson, because the Fourth Amendment is not trapped by a static piece of legislation. “The justices have the benefit of the common law and constitutional law and it evolves,” she explains. “It’s more than much more sustainable to evolution.”

The nation’s highest court is not alone in its efforts to bolster privacy protections. Although federal legislators may be spinning their wheels, state lawmakers have stepped up. While Congress has been mired in inertia, we’ve seen state legislators take decisive action, Wessler says. “Over a dozen states have passed bills on location tracking.”

That momentum, for Wessler, creates a glimmer of hope that the Fourth Amendment might reassert itself and state lawmakers can work together. “We see the shadow cast by national security justifications and corporate interests.”

A more extensive version of this article is available on our website.
The U.S. government’s penchant for data, contractor Edward Snowden exposing changing online habits and possibly accountability.

Privacy concerns

The Data Backlash

Is resistance forming against data-sharing in America? The consensus seems to be a resounding ‘yes,’ reports Ashley Carman.

Americans have questions, and they want answers. Thanks to former National Security Agency (NSA) contractor Edward Snowden exposing the U.S. government’s penchant for data, and recent documents revealing the way law enforcement uses stingray devices to often collect innocent civilians’ data, Americans are pushing their government, technology providers and anyone with access to their data for answers and accountability.

Plus, mounting evidence that living under the threat of surveillance is changing online habits and possibly stifling creativity is now prompting companies to modify products and change their approach to privacy. A pair of Pew Research Center studies illustrates Americans’ privacy woes. Research from November 2014 found that 91 percent of adults “agree” or “strongly agree” that consumers have lost control over how personal information is collected and used, and 80 percent agreed or strongly agreed that Americans should be concerned about the government’s monitoring of phone calls and internet communications.

A second study from March of this year shows just how those beliefs translate into tangible behavior. Twenty-two percent of American adults say that since the Snowden revelations they’ve changed the patterns of their own use of various technological platforms “a great deal” or “somewhat.” That’s not good news for a digital society where personal lives and business thrive on the flow of information, and innovation depends on people having the freedom to explore and work without government peering over their shoulders. While the percentage of people who’ve adjusted their online habits isn’t a majority, it still represents more than 50 million Americans and doesn’t even take into account the vast majority of Americans who are simply aware of government surveillance, or 87 percent of adults.

“These are huge numbers,” says Omer Tene, vice president of research and education at the International Association of Privacy Professionals. They also demonstrate a privacy awareness that “certainly wasn’t the case before the whole Snowden NSA story got out.”

He explains that in the wake of those revelations, American society has seen a “spike in knowledge, awareness and interest from consumers and, correspondingly, from businesses that have to react to consumer sentiment.”

Patrick Eddington, policy analyst in homeland security and civil liberties at the Cato Institute, a public policy research organization, agrees, positing that the world is seeing a “digital resistance movement.”

That resistance is apparent in Citizenfour, a documentary about Snowden’s leaks. When discussing the documents he’s downloaded from the NSA, Snowden takes care to avoid eavesdropping by unplugging his hotel room’s phone. It’s almost cringe-worthy paranoia. While most of us aren’t Snowdents with a specific reason to worry about government surveillance, his concern and care seemed to preview the future of privacy and the lengths to which citizens might have to go to preserve theirs.

With 54 percent of Pew Research respondents believing it would be “somewhat” or “very” difficult to find tools and strategies that would help them be more private online and with their cell phones, duct tape over a webcam can’t be ruled out. But more thoughtful — and feasible — alternatives exist.

The lack of knowledge around privacy options “is an indication that public education needs to take place,” says Eddington. “There are excellent privacy tools out there, and they’re getting easier to use with each passing month.”

For instance, the Blackphone, a privacy-driven mobile device from Silent Circle, features apps, including two that encrypt both phone calls and text messages, that attempt to give users control over their data.

“All of the sudden there’s this manifestation of all those [privacy] fears being realized across what we’re doing,” says Bill Conner, CEO of the Switzerland-based encrypted communica-tions firm. Public discomfort with privacy issues is driving interest in his firm’s platform, he says.

A number of companies beyond Silent Circle are rising up to fill the void where the government and its policies have failed, Eddington says, but even more than new products being created with privacy in mind, companies are attempting to gain back users’ trust with their own privacy deployments. It’s not a surprising move given that 81 percent of Americans feel “not very” or “not at all secure” using social media sites when they want to share private information.

Yahoo, for example, met consumers’ call by saying it would begin rolling out end-to-end encryption for its email users. WhatsApp implemented encryption on users’ messages last year and transpar-ency reports — proffered by the likes of Google, Twitter and Facebook to show data requests from government and law enforcement — have been presented as evidence that social media firms are trying to keep their customers in the know. These companies are focusing on reestablishing relationships with users based on trust as opposed to forcing new ones. To that end, they’re looking into roles beyond a privacy officer.

“It’s evolving into a question of trust,” says J.J. Thompson, CEO and managing director at Rook Security, an Indianapolis-based provider of global IT security solutions. Building “the creation of trust officers who bridge privacy and security and brand under one umbrella.”

This recent change, he says, marks a reevaluation of how enterprises handle data in order to quell employees’ and customers’ concerns and answer lingering questions after Snowden’s revelations.

While a privacy officer might only focus on privacy-related endeavors, trust officers listen to both IT security professionals and the rest of the organization to ensure employees feel safe with a company having their data. They ensure employees have protections in place if data does become compromised, Thompson says.

Because data collection is well underway, organizations must focus on securing it and keeping its exposure to only relevant parties, says Darrin Reynolds, chief privacy officer (CPO) and VP of information security at Diversified Agency Services (DAS), a division of Omnicom Group, a New York-based global enterprise of marketing services and specialty communication companies.

“Instead of worrying about my information getting out, I would rather have a bigger recourse for dealing with situations where information got misused for something I didn’t like,” Reynolds says. “It won’t be about control, but rather, consumer action on corporate accountability.”
A data breach is heating up, reports Lee Sustar.

The battle over who pays what to cover the cost of stolen credit card information is heating up, reports Lee Sustar.

As the costs of the 2013 Target breach hit $252 million on its way to an estimated $1 billion, a federal judge green-lighted a lawsuit by regional banks and credit unions that could push even more of that cost onto the retail giant and set an important precedent for the payments industry.

If the December ruling by U.S. District Court Judge Paul Magnuson in the Minneapolis-based Minneapolis bank’s lawsuit, litigation against Target is settled. Yet the mere fact of its existence could change the balance of power between merchants and financial institutions. Others may be caught in the crossfire. “What we are seeing is that retailers are starting to sue their Q&As (qualified security assessors) to help pay for the cost of data breaches,” says Kurt Hagerman, CSIPO at FireHost, a Richardson, Texas-based secure cloud hosting provider.

Retailers are fighting back
More tensions, conflict and maneuver around these issues are likely in the months ahead as cybercrooks keep at it, says Marcus Christian, a Washington, D.C.-based attorney with Mayer Brown, an international law firm. “Right now you have a situation where it is hard to get your arms around the risk,” says Christian. “Even cyber-insurers don’t have the long history where they will be able to calculate what the losses will be” in the event of a breach.

Soon after his ruling on the banks’ lawsuit, Judge Magnuson also refused to dismiss a separate lawsuit filed against Target by consumer groups. The C-suite is taking note, says Jared Carsten, CSIPO at the international construction firm CRH, and a leading member of the Irish chapter of ISACA. “The liability lawsuits and the loss of customers is shifting the mindset.”

The retailers are fighting back. Big merchant groups claimed that it is retailers who actually absorb the costs of breaches by, among other things, paying for credit card reissuance under the terms of their contracts with Visa and MasterCard. Moreover, if the banks have a beef with their fraud and data breach costs, they have only themselves to blame for their failure to upgrade credit cards to chip-and-pin EMV technology, says Avivah Litan, vice president and analyst at Gartner, the Stamford, Conn.-based consulting firm. They had plenty of time to pay for it as a group when the technology became available eight years ago, she says. “There is a collective responsibility. Banks are more responsible than the retailers because they should have upgraded the technology.”

Amid controversy, IT security vendors must work customers on all sides — not just to find the right technology, says Andrew Plato, president and CEO of Anitian, a Beaverton, Ore.-based provider of security, compliance and risk management solutions. “People have technology fatigue,” he says. “What’s needed, he contends, are the development systems and processes to assess and manage risk, and to clearly establish liability through contracts.

Tiffany Jones, chief revenue officer for iSight Partners, a Dallas-based provider of threat intelligence services, makes a similar point. “If bad guys want to get in and they’re highly sophisticated, they will find a way to do that,” she says. “But if an organization or a company has taken reasonable steps in terms of security architecture and best practices, and have met that reasonableness standard, there needs to be some heady discussion as to where those organizations are still liable.”

Yet, assessing cybersecurity risk — and deciding which party must take on that risk when contracts are signed — remains difficult, says Andrew Braunberg, a research director at NSS Labs, the Austin, Texas-based research firm. There is potential for breaches in the landscape in which merchants may have greater liability, he says. But the issues will likely linger until insurance companies can amass better information. “Let them do their best practices based on actual breach data,” he says.

In this current environment, CISOs and other data security specialists involved in payments will need patience and a long-term perspective, says Mike English, executive director, product development at Princeton, N.J.-based Heartland Payment Systems. “Even merchants and businesses that implement EMV still need to maintain PCI,” he says. “We are not going to see magic go away any time soon.”

While the financial institutions and merchants battle it out in court, the data security industry is attempting to meet the needs of both camps by offering encryption and tokenization technology, English says. “When people implement EMV solutions, the vast majority are migrating to encryption and tokenization at the same time.” That technology, he says, “is going to decrease the number and severity of breaches, and assessments we see in the U.S.”

In the meantime, the breaches keep coming — and whatever technology is in place, the question of who pays may well be decided in a Minnesota courtroom.
I n the strictly monitored biopharma industry, the authenticity of signatures on documents is essential for the smooth operation of clinical trials. With 150,000 registered clinical trials currently just in the United States, according to the U.S. Department of Health & Human Services, biopharma companies are electing to complete digital signatures through the use of the company’s cloud digital signing services, Schmidt explains.

The search began for a solution that would enable customers to optimize this task and ensure secure transactions. SureClinical’s executive, security and engineering teams worked together on an extensive review of available options, says Schmidt. First his team set up requirements around what was needed. The system had to have FIPS-140 Level 3 high-trust security for storage of credentials. It had to be a hardware security module (HSM). His team also required the ability to support millions of signing transactions a day, so the hardware had to support big amounts of throughput as well as the ability for failover and very high reliability.

“One of the key things we needed was a mean time between failure on the order of hundreds of thousands of hours,” Schmidt says.

He also needed something in the cloud that could scale with the growth of the organization. As his team added new users, the solution needed to be able to scale gracefully. “Our users needed the ease and convenience to be able to access the solution and start signing securely right out of the box, and to do it from familiar tools, like a mobile phone,” Schmidt says.

Another thing that was important was support for APIs. The flexibility and support for different kinds of programming languages was critical. Schmidt’s team looked at a number of options but had concerns. USB solutions were unacceptable for doctors. “No one wants a USB device that plugs into his or her laptop for signing,” he says. The team looked at another solution which, Schmidt says, was good but not as reliable as what was needed. Plus, it lacked the capability to scale the way Schmidt and his team required.

Then they discovered the Thales nShield HSM. “The Thales unit was the only unit with the mean time between failure we needed, and for support for millions of users and millions of transactions. It superseded everything. We were really happy to find that solution.”

At the heart of any digital signing infrastructure is secure private key storage, Schmidt says. “We use the Thales HSM nShield technology to store signing keys for the identities of individual medical investigators, so the investigators can securely sign clinical trials documents from mobile or web devices.”

The HSM maintains all private keys and identity credentials in secure, tamper-resistant devices that allow SureClinical’s security team to guard both the validity and the security of the investigators and document signatures that are created on their behalf. “That’s absolutely paramount to this industry,” he says.

Zack Schmidt, founder, president and CEO, SureClinical
president of product strategy, Thales e-Security, with U.S. headquarters in Palm Beach Gardens, Fla. “Keys need to be locked down with rigorously enforced access controls and usage policies and yet be available in use at the center of the business service, signing and exchanging documents in the case of SureClinical. As a result, ease of deployment and security can become two opposing forces.”

With the Thales HSM, Schmidt’s team is able to provide an identity around a digital signature that is pre-verified and pre-approved through the use of a PIN code and a cell phone. “We have the strongest level of digital signing,” he says. “In fact, as far as we know, we are the only organization that’s been approved for Adobe digital signing from a mobile device.”

“The Thales HSM, we’ve been able to establish the highest level of security in the cloud and make it accessible from a mobile phone, including an additional layer of security provided through SMS.” Users get a verification code assigned through their mobile device, so instead of having to carry around a USB device that can be easily lost, investigators now just have to have a mobile phone to access a signing service in the cloud. The beauty of having a solution in the cloud is that you can validate identities across your entire installed base automatically, Schmidt says. “Companies are required by law to go through extensive validation of their technology, which can add tens of thousands of dollars additional validation. Using the Thales HSM, we were able to validate this once across a certified cloud by default.”

Schmidt and his team were impressed with the Thales pre-deployment support. “They spent time explaining alternative approaches of configuration and deployment in data centers and different security settings that we could use,” he says. “We were also impressed with their assistance with the initial programming of the unit for the API interfaces we use with Java. The team’s expertise was top-notch overall.”

When equipment is deployed, it can be an expensive and time-consuming undertaking, he says. “It really helps to have somebody help you set it up, prove it, prototype it and pilot it before you put it in production. That’s what Thales did with us, which was really great.”

And, Schmidt is finding that implementation easy to manage and operate. “We’ve had no issues at all,” he says. “It’s been plug-and-play since that initial configuration and setup.”

The Thales security tool stretches across SureClinical’s entire network. “SureClinical is already in the 15 to 20 different countries where people are digitally signing documents, and we can scale out of the box to 130 countries overall,” Schmidt says. Further, SureClinical is expanding its digital signing to include providing trusted identities for health care pros. So, when customers sign up a clinical trial, they can tap into its database of providers with a trusted identity through the Thales HSM unit. This is going to help vet doctors and investigators for clinical trials. “Think of it as a highly trusted LinkedIn where the trusted individual has an identity that is held within the Thales unit,” Schmidt says.

As health care and life science applications shift away from paper and to the cloud, trust is a key element of making it successful. “Thales HSMs provide the trust that empowers our customers and facilitates their move to the cloud,” says Moulds.

DOCTOR’S ORDERS Rx for digital signing
Thales supplies a security platform known as a hardware security module (HSM), says Richard Moulds, vice president of product strategy at Thales e-Security. “These devices act as a root of trust for a wide range of applications that employ cryptography to protect documents, sensitive data and business services.”

SureClinical handles thousands of highly sensitive documents that contain medical records and data from pharmaceutical trials and uses cryptography to ensure privacy and digital signatures to validate the authenticity of documents, Moulds explains. The Thales eShield HSMs protects the secret keys at the heart of the process and performs the critical signing operations, he says.

SureClinical faced the challenge of building an application infrastructure that was sufficiently scalable and had global reach to provide a reliable alternative to sending physical documents by traditional postal services, Moulds says. “The only way to achieve this was for SureClinical to develop a highly secure cloud-based service. The high performance and tamper-resistant capabilities of the shielded HSM was perfectly suited to SureClinical’s requirements and enabled it to obtain the federal security certification that is necessary to process pharmaceutical records.”

These devices act as a root of trust...
– Richard Moulds, VP, Thales e-Security

UTM, SIEM. What’s the dif?
Several years ago, I started writing about universal threat managers, also called unified threat managers. In those days, they were a sort of evolution of several types of gateways. Their purpose was to actively manage threats. Typically, these devices included firewalls, VPNs, IPS, URL filters, DLP, anti-spam and anti-malware. The gateways evolved from point solutions to posture problems and, in effect, simply pulled all of the pieces together in a single system.

The UTM market continues to grow in the double digits year on year, according to Forrester. Along the way, other technologies — such as load balancing and integrated endpoint security — have gone a long way toward easing my pain relative to these tools. I guess, in that regard, I’m ready to cry “uncle.” I no longer wonder to see if UTM is “soup-yet.” They assuredly are. Which brings us to SIEMs.

SIEMs are another evolutionary product — an amalgam of SIM (security information management) and SIEM (security event management). Those original have not been around for a long time. The amalgam took off like a flash, eclipsing the older approaches. And for very good reason: information and events go together closely in the cyber event management world. It makes sense to keep the two together. But, it is important to remember that SIEMs do not create their own data. They consume other data and analyze, and report on that data. So, SIEMs — and should — take the role of alerting. So the SIEM becomes the point of aggregation. It aggregates information from a variety of sources and manages the events sent to it.

Today’s SIEMs can do things with data feeds that just a few years ago seemed like science fiction. Imaging gathering data streams from a variety of sources, stripping out indicators of compromise and using that information — along with some additional data — to identify a known threat actor. So, it is clear that these are two entirely different beasts. But do we need both? If we’re talking about my network, yes we do! On your network, your mileage, as they say, may vary. But I certainly would want both for protection and knowledge of what is happening on an increasingly complicated enterprise. So, that is the theme this month — SIEMs and UTM and where they fit into your enterprise. Our review team this month was Ben Jones, Sal Picheria and James Verderico. Nice job, team!

– Peter Stephenson, technology editor

How we test and score the products
Our testing team includes SC Labs staff, as well as external experts who represent the viewpoints of our Group Tests. We look at several products around a common theme based on a pre-defined 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 5400) 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 shown in a specific area.

Lab Approved is awarded to extraordinary standouts that fill into the SC Labs environment, and which will be used subsequently in our test bench for the coming year.
The main purpose of the SIEM is analysis. UTMs generate data from events they are intended to monitor. You likely need both, says Technology Editor Peter Stephenson.

Let’s start out by saying that the SIEM and UTM tools are not mutually exclusive. You can – and should – belong to both. The histories of these two tools are, actually, quite similar. Both came from the concatenation of several point solutions to point problems.

In the case of the SIEM, it was the joining of security information and event management. In the UTM, it was grouping a number of tools together that conveniently fit into a single appliance. Typically, the appliance was located on the perimeter of the enterprise. The functionality of these two types of appliances – and they can be physical or virtual – has grown to keep pace with the times, but they still have two defining differentiators: SIEMs consume data from multiple external sources while UTMs develop their own data from various forms of monitoring.

We start with SIEMs because they are the easiest to place in the architecture of the typical enterprise. The main purpose of the SIEM is analysis. Different SIEMs use the analysis in different ways but, at their cores, SIEMs take in a lot of data from multiple sources, normalize it and correlate it so that conclusions can be drawn and decisions made. The key – or, at least, the first key – to SIEM functionality is normalization. This means that the SIEM must be able to consume whatever kind of data you want to feed it. It is not enough, of course, simply to consume the data. Once consumed and normalized – placed into a format that the SIEM will find consistent with other consumed data – the SIEM can analyze.

Normalization consists of parsing the consumed data into chunks that are meaningful in the context of the SIEM’s analysis functions. So if the only thing the SIEM can consume is syslog format, you have a problem. Data comes into the device in a variety of formats and not all of them are syslog. This usually means that the manufacturer will, at some point, need to write a custom connector for some obscure data format brought to it by a customer. If your SIEM manufacturer can’t – or won’t – do that, you have the wrong product.

However, most SIEM manufacturers will, and most have very large collections of pre-written collectors. The collectors may be called something else, such as interfaces, but their purpose is to parse the data from a particular source into useful chunks. SIEMs take the normalized data and correlates it so that they have a complete picture from the perspective of every device connected to them. That means that they “connect the dots” between the firewall, IDS/IPS and any other log-producing devices on the network. The more data points a SIEM has, the more useful it becomes. Finally, the SIEM makes something useful out of all of the data points.

UTMs, on the other hand, generate data from events that they are intended to monitor. A UTM might be an excellent feed for a SIEM. UTMs do not just generate data, either. Some UTM functionality is aimed at such things as providing VPN service. Here is where it can be difficult to select a UTM product. If you are not using a UTM at the moment, you probably have many of the point solutions to individual challenges. So, for example, if you are running a VPN already, does it make sense to buy a UTM that also provides a VPN? Actually, it might. Depending on the other functionality – and how much redundancy it has with tools that you have already – it may make perfect sense to buy the UTM and turn off the unneeded functions. In many cases, the UTM offers several advantages over those point solutions.

First, it likely is easier and more efficient to administer the UTM than a bunch of individual tools. Ease of administration translates into efficiency and that translates straight to your bottom line. Also, there are benefits to seeing the bulk of your security environment in a single pane of glass. Again, more efficiency is better.

So, the bottom line? You likely need both SIEM and UTM, and just because you have point solutions does not mean that a good UTM is out of the question for your enterprise.

Eratum: On page 42 of the April issue we misidentified LoginTC from Cyphercor. The vendor name should be spelled Cyphercor (rather than CypherCor) and the vendor should be Cyphercor (not LoginTC). Our apologies for the errors.

**PICK OF THE LITTER**

Intel Security’s McAfee Enterprise Security Manager is a security information and event management suite. It is the gold standard for your enterprise.

WatchGuard Firebox M440 is truly an excellent choice for a UTM device. We select this UTM tool as Recommended.
The AlienVault Unified Security Management platform is one of the most unique products we have ever had the pleasure of reviewing. Off the bat, it comes in for this review cycle as the least expensive hardware SIEM. The price is nothing to go by, however. This device comes with some of the most advanced functionality of any SIEM we have seen. It is available as a preconfigured VM, an Amazon cloud appliance, or as a hardware appliance like the one we received. The setup phase of our examination went flawlessly. We removed the tool from the box, racked it up and hooked up our mouse and keyboard. Then, we connected it to power and turned it on. After it booted, we were greeted by a wizard-based onboard setup program to configure the basic settings. We configured the management interface, applied our settings and waited for the device to reload. It then prompted us to complete setup from a web browser. We fired up an SC Lab PC, connected to the AlienVault and proceeded to finish the install. Once we logged in, AlienVault redirected us to its built-in setup. We followed the wizard to import our license, change the password and create an account with AlienVault. Lastly, we configured the remaining interfaces and let it scan our network for devices. One of the USM’s greatest features is its GUI. As far as management consoles go, this device takes the cake for the absolute best graphical interface we have seen. The tool is not just a SIEM, it also happens to have a work of art sitting inside waiting to be painted with your network logs. Every single page is customizable and interactive, making it incredibly easy to understand and use. The data collected by AlienVault is displayed and categorized with more charts, graphs and maps than any other product we reviewed. The USM not only analyzes logs, but it also can be configured to monitor a network tap and scan for unusually high volumes of traffic or other anomalies and report on those as well. Through a program called OTX, customers can choose to anonymously send threat data to AlienVault in exchange for the global collection of data generated by the rest of the participants. This is brought directly into the management console and provides valuable insight into malicious activity by IP and region.

For support, AlienVault offers the option at a cost of approximately 30 percent of the purchase cost. Its hours are unique: eight-hours-a-day/five-days-a-week. NGTP setup was superb. We plugged it in, plugged in the nearest computer with a web browser, and were greeted by a “change the password” box, no default password to look up. We had this UTILITY running in under three minutes. We never once had to look at the documentation during setup, and everything was intuitive. This may have been the easiest product we have ever set up. Check Point NGTP has integrated VPN and SSL VPN and this too was simple to set up. It has integrated Wi-Fi, including virtual access points, to host more than one Wi-Fi network; for instance, a guest Wi-Fi. It has simple checkboxes to block security risks, inappropriate content, file-sharing applications and an extensive list of other applications, logging all blocked traffic and syncing that data with users or network devices gathered either manually or through Active Directory. NGTP allows for cellular modern and even an express card slot for cellular networks.

The real-time logging was pleasant to look at and sending system logs to external servers is a click away. We found it easy to search through thousands of logs, look for hosts infected with malware based on the traffic they have, and even see which ports different machines on the network were currently using. We were able to quickly see the bandwidth services and applications were using, and NGTP was able to sort through the applications at higher risk and even tie that to a username. Generating reports was easy. Like everything else with this device, it was quick and effective and the report generated was simple, beautiful, understandable and useful. This offering was so intuitive, we found ourselves looking at the documentation only after conducting most of our review. The documentation is clear, filled with screen shots on nearly every page as well as step-by-step instructions with explanations. Even though we didn’t need it, the manual was extremely well made.

Check Point offers three different support options: Standard, for $228, which includes nine-hours-a-day/five-days-a-week with, a response time of four hours; Premium, for $323, and Elite, for $380. Both offer 24/7 support with a 30-minute response time. The difference between Premium and Elite is that Elite has more options for onsite aid.

Check Point Next Generation Threat Prevention Appliance was one of the best tools we’ve seen, for a price that can’t be beat. It was easy, solid, stable and it had an impressive feature set. We have no hesitation in giving this product our Best Buy designation. – SP

**Check Point Software Technologies**

**1180 Next Generation Threat Prevention Appliance**

The real-time logging was pleasant to look at and sending system logs to external servers is a click away. We found it easy to search through thousands of logs, look for hosts infected with malware based on the traffic they have, and even see which ports different machines on the network were currently using. We were able to quickly see the bandwidth services and applications were using, and NGTP was able to sort through the applications at higher risk and even tie that to a username. Generating reports was easy. Like everything else with this device, it was quick and effective and the report generated was simple, beautiful, understandable and useful. This offering was so intuitive, we found ourselves looking at the documentation only after conducting most of our review. The documentation is clear, filled with screen shots on nearly every page as well as step-by-step instructions with explanations. Even though we didn’t need it, the manual was extremely well made.

Check Point offers three different support options: Standard, for $228, which includes nine-hours-a-day/five-days-a-week with, a response time of four hours; Premium, for $323, and Elite, for $380. Both offer 24/7 support with a 30-minute response time. The difference between Premium and Elite is that Elite has more options for onsite aid.

Check Point Next Generation Threat Prevention Appliance was one of the best tools we’ve seen, for a price that can’t be beat. It was easy, solid, stable and it had an impressive feature set. We have no hesitation in giving this product our Best Buy designation. – SP

**Check Point Software Technologies**

**1180 Next Generation Threat Prevention Appliance**

The real-time logging was pleasant to look at and sending system logs to external servers is a click away. We found it easy to search through thousands of logs, look for hosts infected with malware based on the traffic they have, and even see which ports different machines on the network were currently using. We were able to quickly see the bandwidth services and applications were using, and NGTP was able to sort through the applications at higher risk and even tie that to a username. Generating reports was easy. Like everything else with this device, it was quick and effective and the report generated was simple, beautiful, understandable and useful. This offering was so intuitive, we found ourselves looking at the documentation only after conducting most of our review. The documentation is clear, filled with screen shots on nearly every page as well as step-by-step instructions with explanations. Even though we didn’t need it, the manual was extremely well made.

Check Point offers three different support options: Standard, for $228, which includes nine-hours-a-day/five-days-a-week with, a response time of four hours; Premium, for $323, and Elite, for $380. Both offer 24/7 support with a 30-minute response time. The difference between Premium and Elite is that Elite has more options for onsite aid.

Check Point Next Generation Threat Prevention Appliance was one of the best tools we’ve seen, for a price that can’t be beat. It was easy, solid, stable and it had an impressive feature set. We have no hesitation in giving this product our Best Buy designation. – SP

**Check Point Software Technologies**

**1180 Next Generation Threat Prevention Appliance**

The real-time logging was pleasant to look at and sending system logs to external servers is a click away. We found it easy to search through thousands of logs, look for hosts infected with malware based on the traffic they have, and even see which ports different machines on the network were currently using. We were able to quickly see the bandwidth services and applications were using, and NGTP was able to sort through the applications at higher risk and even tie that to a username. Generating reports was easy. Like everything else with this device, it was quick and effective and the report generated was simple, beautiful, understandable and useful. This offering was so intuitive, we found ourselves looking at the documentation only after conducting most of our review. The documentation is clear, filled with screen shots on nearly every page as well as step-by-step instructions with explanations. Even though we didn’t need it, the manual was extremely well made.

Check Point offers three different support options: Standard, for $228, which includes nine-hours-a-day/five-days-a-week with, a response time of four hours; Premium, for $323, and Elite, for $380. Both offer 24/7 support with a 30-minute response time. The difference between Premium and Elite is that Elite has more options for onsite aid.

Check Point Next Generation Threat Prevention Appliance was one of the best tools we’ve seen, for a price that can’t be beat. It was easy, solid, stable and it had an impressive feature set. We have no hesitation in giving this product our Best Buy designation. – SP

**Check Point Software Technologies**

**1180 Next Generation Threat Prevention Appliance**

The real-time logging was pleasant to look at and sending system logs to external servers is a click away. We found it easy to search through thousands of logs, look for hosts infected with malware based on the traffic they have, and even see which ports different machines on the network were currently using. We were able to quickly see the bandwidth services and applications were using, and NGTP was able to sort through the applications at higher risk and even tie that to a username. Generating reports was easy. Like everything else with this device, it was quick and effective and the report generated was simple, beautiful, understandable and useful. This offering was so intuitive, we found ourselves looking at the documentation only after conducting most of our review. The documentation is clear, filled with screen shots on nearly every page as well as step-by-step instructions with explanations. Even though we didn’t need it, the manual was extremely well made.

Check Point offers three different support options: Standard, for $228, which includes nine-hours-a-day/five-days-a-week with, a response time of four hours; Premium, for $323, and Elite, for $380. Both offer 24/7 support with a 30-minute response time. The difference between Premium and Elite is that Elite has more options for onsite aid.

Check Point Next Generation Threat Prevention Appliance was one of the best tools we’ve seen, for a price that can’t be beat. It was easy, solid, stable and it had an impressive feature set. We have no hesitation in giving this product our Best Buy designation. – SP
CorreLog
SIEM Correlation Server v5.5.0

The CorreLog SIEM Correlation Server is a flexible solution for strengthening security on a network. The product comes packed with great tools and functionality that allows customers to ensure proper log collection. The solution combines real-time log management with correlation, automation functions, high-speed search, ticketing and reporting services.

The server's installation and configuration process was simple. The product was sent to us on a DVD containing a Zip of the application, as well as all necessary documentation in PDF format. Once we offloaded the content of the DVD onto our desktop, we downloaded the file and began the installation. The total installation took no more than four minutes and was simple to follow. Once the installer finished, we began installing the Windows Syslog Agent Package onto our other computers in order to start log data collection and data correlation.

This SIEM solution is extremely versatile, seeing as the server is capable of managing upward of 2,000 messages per second and traffic bursts of more than 10,000 messages a second. The CorreLog server uses “semantic correlation” that makes use of correlation counters, alerts and triggers to help reduce incoming messages into something understandable. This extremely flexible software provides users with rapid compliance standard auditing (PCI DSS, HIPAA, GLBA, etc.). CorreLog provides the ability to strengthen threat detection and security management as a whole on a small, medium or even large enterprise-level network. The actual software, once installed, is easily controlled through the web GUI. The easy-to-use interface provided us with fluidity when displaying collected data, managing alerts and tickets, as well as generating reports. The large number of analytical features provide unique insight into user and system behavior and anomaly detection. The tool also supports syslog data from a plethora of operating systems, hardware devices and applications and it even can integrate with anti-virus monitoring.

The documentation is straightforward and provided us with more than enough information to get the product fully functioning. The “CorreLog Correlation Reference Manual” is a useful document that provided us with explanations for a variety of functionality and terminology the software uses to correlate data.

This comprehensive SIEM solution can provide the necessary strengthening to a network. Its vast customization options can provide security analysts with the necessary “depth” of data they need, in order to suit the requirements on their network. Overall, this product is a great choice for a SIEM solution on a network and should definitely be considered when looking for a trusted SIEM application.

Cyberoam Technologies
CR1000iNG-XP

Cyberoam CR1000iNG-XP is a next-generation firewall appliance that includes VPN, email, anti-virus, HTTP and HTTPS and FTP anti-virus, anti-spam and IPS with custom signatures inside the modular appliance. Cyberoam is extremely versatile and expandable with room for four additional modules on the appliance and license subscriptions to enable different features.

Cyberoam setup was incredibly easy. It was plug and play. We put it in the rack, ensured we could connect and connecting to it internally required minimal effort. Web filters are a simple set of checkboxes and quality of service (QoS) is the same. Setting IP through a console cable or the push button GUI found on the faceplate was easy. Cyberoam was pre-configured to automatically do all of its base functionality out of the box. The only real configuration needed was when we wanted to access some of the more advanced features.

The tool's VPN has a slew of options: SSL, VPN, IPSec, PPTP, L2TP and Cisco VPN Client. Cyberoam also includes denial-of-service (DoS) prevention into the firewall, anti-virus and email security. It keeps traffic logs and can create compliance reports.

Cyberoam CR1000iNG-XP allows for high availability – a must for any enterprise environment. It can identify attacks and their severities according to your environment. Setting up rules for a web app is easy as well, with sets of pre-configure rules and the ability to QoS different applications and web filters on networks with a level of granularity that is unique. We credit Cyberoam with some of the best scalability. Modules called FlexXi ports enabled scaling between 10 and 42 ports on the particular model sent to us. Up to 42 ports enables some creative networking solutions and proper network segmentation that may not always be possible with some other next-generation firewall appliances.

Cyberoam sent us extensive documentation. It was clear and screen shots helped us better understand the deployment. However, the product was easy enough to use that we rarely needed to reference it.

Support options include eight hours a day/ five days a week through phone, email and web chat, with firmware upgrades and hardware warranties at $2,795 per year. 24/7 support is $3,445 per year. Cyberoam also offers a number of subscription types that include feature sets, including anti-malware filters, anti-spam, web and application filters, IPS and packages combining features sets as well.

Cyberoam Technologies CR1000iNG-XP is a comprehensive suite of tools designed to save the administrator time. Everything is straightforward. One caveat: Though it works well enough, for the money, we expected a little more out of it. However, Cyberoam has some of the best expandability in the market, so we recommend it for large-scale deployments and for businesses that are growing rapidly.

**GROUP TEST SIEM/UTM**
**Dell SonicWALL NSA 3600**

The Dell SonicWALL NSA 3600, along with its TotalSecure license bundle, is the company's offering for the UTM gateway and next-generation firewall market. This dynamic duo is a security powerhouse packed into a 1U rack mount server. It offers some of the best high-security features we have seen, while still remaining user-friendly and intuitive. The NSA 3600 offers a good balance of features making it a good fit for single- or multiple-hundred-unit deployments.

We started by removing the tool from the box. We racked it up and then headed over to the quick-start guide to figure out how to connect the LAN and WAN interfaces. Once we connected those, we headed to an SC Lab PC and continued setup with a web browser. The folks at Dell loaded up our licenses for us, but we still had work to do to complete our install. We opened up the built-in quick setup menu, where we configured the time, WAN interface and other environment settings.

After the device was set up, we began experimentation with some of the many security features offered by our license set. We breezed through the configuration of the security features as if we had been doing it for years, despite the fact that we had never used the product before. The interface was well designed and easy to pick up. One feature we really liked was the Dell Threat Report. Dell provides users with global data about popular threats and makes it available from within the device internal to the enterprise, and then that data can be exported in an executive-friendly PDF report.

The NSA 3600 also has built-in support for cellular failover WAN, as well as WLAN control for SonicWALL access points. Speed is particularly emphasized on this model, with support for wireless AC and two 10Gbe QSFP+ ports standard.

Dell SonicWALL products come with a 90-day software support period and a one-year hardware warranty factored into the cost. This provides customers with access to telephone, email and web support, as well as software updates. Most customers will want to extend the duration of support and Dell offers extension packages in eight-hours-a-day/five-days-a-week and 24/7 variants for between one and six years.

The Dell SonicWALL NSA 3600 is an excellent choice for medium to large organizations desiring easy management of many devices from one place. It offers the raw power and throughput to support organizations of this size, but these features will likely go unused at smaller organizations. Growing organizations will also be able to make good use of the performance features of the NSA 3600 because they can use a gigabit now and then grow into 10-gigabit later as the network requires. – SP

---

**Siemens SecureVue**

The Siemens SecureVue software suite is a comprehensive log and asset management system that lets network administrators quickly get the full picture of what is going on in their network. It is an extremely robust and powerful tool which takes some time to master, but after getting acquainted it becomes easy to navigate and provides a deeper level of log management and analysis than is usually found.

We received the SecureVue system as a preconfigured hardware appliance. We did the usual: removed it from the box, racked it up and connected power. We connected the keyboard, mouse and monitor before powering it on and then waited for it to boot up. After that, we configured the network settings through the Windows server GUI and then followed EiQ’s steps to reconfigure the software suite’s IP. The setup was rather involved, but went smoothly and without incident. EiQ loaded our licenses for us, and the time was already correct, so after logging in with the built in administrator account we changed the password to finish setup.

After setup was done, we used an SC Lab PC to connect to the SecureVue’s web interface. We were greeted with a slew of graphs and charts, but it took us a considerable amount of time to get the whole system running. Because it is so powerful, it takes a lot of configuration to leverage the advanced feature set of this device. Once it is configured, SecureVue is capable of correlating logs from basically every networkable device available. Once the logs are collected, they can be forensically investigated by easily searching the system for triggers, assets or events. SecureVue is even capable of integrating with popular vulnerability assessment systems for single-screen vulnerability and threat analysis capability for managed assets. Out of the box, SecureVue comes with templates to view alerts from devices, templates to check those alerts against compliance mandates, and even more templates to customize how they are displayed to the user. Once it is set up, SecureVue is a powerhouse for prioritizing security response.

All of the documentation was well written, easy to understand and contained pictures and screen shots where appropriate. EiQ includes one year of standard support with the purchase of the SecureVue system. Standard support includes eight hours a-day/five-days-a-week telephone, email and web support. This can be extended for the price of 20 percent of the product. Premium support is also available.

Even though it is pricier than other alternatives, we find EiQ Networks SecureVue to be a good value for the money. It is highly customizable and combines traditional SIEM functionality with advanced passive vulnerability scanning to give administrators more control over their network. – SP
The EventTracker Security Center v7.6 is a great solution for enterprise security information and event management (SIEM). EventTracker does not offer a preconfigured hardware appliance, but the product is available for deployment either as a preconfigured VM or a standalone installer for custom installation. Virtual appliances are available for both Hyper-V and VMWare. The solution has shown significant growth since its v7.5 release, as it now includes full integration of external threat intelligence with internal threat analysis. The comprehensive functionality of this software allows for a security team to properly and effectively develop risk management strategies and policies to help mitigate network incidents.

The tool was easy to set up. It was sent to us on a USB stick containing all necessary documentation and installation wizards to get the installation going. We installed and configured the software using the provided installers on Windows Server 2008R2 in under an hour. The installation and configuration guides were streamlined and extremely easy to follow. Once the installers finished we were easily able to integrate the full functionality of EventTracker with our network and start the testing.

Although we decided to completely set up and configure Security Center v7.6 with our network, EventTracker provides free initial configuration and tuning for all customers. Once installed, it compresses and stores logs on flat files with a 92 percent ratio compression rate that allows for easy retrieval. The use of a flat file database, consequently eliminates the need for a database administrator and allows non-experts to easily take advantage of the software’s storage functionality. The product integrates with both external threat intelligence (SANS Top 20 Attackers, Spamhaus, Mal0de, etc.) and internal threat intelligence (behavior anomalies, process whitelisting, IP internal whitelisting, internal blacklisting) to provide real-time threat dashboard, alerts and analytics. This allows for an unknown process that occurs internally to correlate with real-world data, such as communication with known malicious addresses.

All guides are easy to read and provide clear screenshot for most of the steps necessary. Clients are offered either a basic no-cost or a fee-based support option. The basic includes access to 8/6 phone and 24/7 email support, as well as a knowledge base on the website. The fee-based option provides the option of a partial weekly or full daily managed service. The web interface proves that this isn’t necessarily true. The web interface on LogRhythm Security Intelligence Platform is stunningly intuitive, customizable and the fastest one we’ve used. It supports more than 700 log types and scriptable parsing to other logs just as in case users need to send other logs to it.

LogRhythm also allows scriptable responses to events and correlated events, including killing processes or raising a ticket to higher tiers of analysis for manual approval of killing that process. LogRhythm’s AI engine can also take a known sterile machine and establish a baseline – critical for point-of-sale-type systems – and provide alerts for processes that don’t fit into that sterile model.

We were impressed with the offering’s forensic abilities and its capability to drill down into logs, search them along multiple parameters, and continue working while it looks through potentially hundreds of thousands of logs without slowing down the interface. Everything about LogRhythm’s interface saves users time or makes it easier.

Documentation was all easily accessible online. There is a guide to do just about everything, though they do not have quite as many visuals as we’d like to see. However, they are clear and concise with step-by-step procedures to get anything done.

Standard support and maintenance includes all software updates, including major and minor releases, and hardware warranty support for three years. Phone aid is accessible from 7 a.m. to 7 p.m. MST, and a 24/7 support portal is available. Platinum includes everything from standard support and 24/7 phone and email support.

LogRhythm is one of the most configurable and automation-ready solutions we tested. It is certainly one of the quickest, empowering the analyst with all the data they could want. Once set up, LogRhythm is without a doubt one of the top products here. If you have a need to dig deep into your logs, while never losing sight of the big picture, LogRhythm may be the product for you. – BJ

---

**EventTracker Security Center v7.6**

**LogRhythm Security Intelligence Platform**
ManageEngine
EventLog Analyzer v10.0

The EventLog Analyzer from ManageEngine is quickly installed and easily scalable software that can be implemented for a network’s SIEM solution. The product is readily available through both purchase and download allowing for rapid installation. It provides both an agent-based and agentless SIEM software that will give a network security team ease of mind. The vast customization and implementation possibilities allows admins to effortlessly monitor logs and simultaneously meet compliance standards.

EventLog Analyzer was extremely easy to setup. The product was shipped to us on a USB stick that contained all necessary documentation as well as a 32-bit and 64-bit Windows installer and a Linux-OS based installer. Once we placed the USB stick into our computer and moved the installer application onto our desktop, we executed it with administrator privilege. Once the installer was executed, we were prompted with two-choices: an advanced-installation button and a one-click installation button for default installation.

The product has an easy-to-use interface which allowed us to set up, configure and then easily begin managing logs in under five minutes. Once the installation was complete, we logged into the web GUI and began adding assets to integrate the software with our test network. A great relief to us was that the software’s out-of-the-box support for a variety of log sources consisting of Windows infrastructure, databases, web stacks, network devices, hypervisors, cloud infrastructure and others. The software is also capable of running more than a thousand compliance reports for event logs and syslogs once manageable assets are added. The compliance reporting section also provides the user with a great amount of customization for report generation with an easy-to-use interface. The analyzer’s “log archival” functionality not only meets the compliance requirements for collected logs, but it also secures them by hashing and time stamping the logs.

Support is offered either as no-cost or fee-based solutions. However, the no-cost option only lasts during the product evaluation period. During that time, full email-, telephone-and web-based assistance is offered on an eight-hours-a-day/five-days-a-week basis. The fee-based option are made available starting at $1,748, but escalate depending on the number of log sources.

Overall, the EventLog Analyzer can provide a hassle-free and altogether effective solution for SIEM on one’s network.

McAfee, part of Intel Security
Enterprise Security Manager (ESM)

Intel Security’s McAfee Enterprise Security Manager (ESM) is a security information and event management suite. It is available as a VM or hardware appliance and supports a massive number of products to produce useful information for security administrators.

We received the VM version. We were sent a download link to the virtual appliance, which – with no additional setup – was deployed to our hypervisor. After giving it an IP address, all that was needed was pointing syslog and other supported devices toward the receiver and from there the logs were correlated. Adding Active Directory is as simple as plugging in account credentials and the IP address of the domain controller, no agent install is necessary: ESM will pull logs through Windows Management Instrumentation (WMI) on an interval set by the user.

The product does everything one would expect a SIEM to do: collect logs across a wide range of devices and integrate with Active Directory. The receiver pulls all the logs in and they are all easily available to the user. Its permissions and user account control makes it easy to limit access to only what certain users need to see.

What really sets the tool apart though is its advanced correlation engine. The deductions made are absolutely astounding. ESM makes correlating different sources and finding outliers, suspicious events and general oddities in the network as easy as can be. Minor outliers can stand out like a sore thumb to the ESM, which makes it extremely useful for quickly and easily tracking down security events and policy violations. The drilldown view allowed us to see the exact logs that caused the alarm or event, enabling the system administrator to decide if the event is worth chasing down.

Documentation includes an extensive list of supported products and syslog parsers, although some information was a bit harder to find than we would have liked. Still, the documentation was good and up to the quality we have come to expect from this company.

There are two support options: McAfee Enterprise Technical Support and McAfee Business Technical Support. McAfee Enterprise Technical Support assigns a single point of contact, called a Support Account Manager, who will visit onsite up to twice per year. All support contracts are 24/7 via telephone. McAfee Enterprise Security Manager has in the past been the gold standard for enterprise grade SIEMs, and it still is. McAfee Enterprise Security Manager provides some of the most useful inferences and information, while not being bogged down by frequent false alarms or wild guesses. It is not the least expensive option out there – at nearly 10 times the price of the least expensive SIEM we reviewed this month – but if you have the money to spend, there is nothing better out there. – BV
Netikus
EventSentry v3.1.1.29

The EventSentry from Netikus brings to the table a plethora of functionality to ensure system security. It is shipped at a more than affordable price point. The product not only provides log monitoring, but also serves as a complete system monitoring suite. The unified threat management software ships with a price depending on the number of licenses per host, as well as other hardware integration for environment monitoring (i.e., temperature sensor, humidity sensor, smoke sensor). The in-depth functionality and limitless capabilities for complete system monitoring makes EventSentry an extremely competitive product when combined with such an attractive price point.

The item was extremely easy to set up. The software, along with all necessary documentation for installation, was sent to us on a USB stick. We opened the drive and ran the setup application using the native installation wizard. After a few clicks and determining the necessary packages for installation, the installation finished and initial setup was done. We then pointed the software to the license key and were then ready for configuration. The initial setup and configuration of EventSentry in its entirety took less than 30 minutes, allowing us to jump right into testing.

While the product offers a variety of complete system solutions, its backbone is its real-time event log and SIEM monitoring component. The software also easily integrates with external hardware that is geared to monitor the environment of your system and will generate alerts for dangerous situations that may arise (increase in temperature, humidity, etc.). A very neat aspect to EventSentry is its thresholding functionality, which allows users to customize the threshold for what may be a network anomaly (such as the amount of failed login attempts considered normal). EventSentry makes use of a central database to consolidate and store logs with the following supported databases: PostgreSQL, MS SQL, MySQL and Oracle. Reports are highly customizable and can easily be filtered, exported (HTML, PDF, CSV) and generated. Scheduled reporting allows for an up-to-date and readily accessible documentation of information security content.

The tool shipped with all necessary documentation to get users from start to finish. The setup, overview and help guides provided us with an easy walkthrough for setup and configuration as well as navigation through the product once installation was finished. The EventSentry is a powerful tool that can be used to monitor and ensure security for the entirety of one’s systems while the admin is away from them. Overall, we were extremely impressed with EventSentry’s data collection and alerting system, as well as the customizable dashboard used to display gathered data. For the price point and software functionality, EventSentry is well worth examining. – JV

NetIQ
Sentinel v7.3

The NetIQ Sentinel may be one of the best SIEM solutions for your network. The vast functionality and comprehensive analysis that this product offers is exceptional measured against how easily it can be integrated into your network. The scalability and wide availability of deployment options makes NetIQ’s product stand out, so long as you have the hardware to support the functionality of a large-data pool.

Sentinel was simple to set up and integrate with our network with no downtime at all. The product was shipped to us as a preconfigured virtual machine on USB stick. Once we unzipped the OVF server template, we deployed it to our hypervisor to begin testing. The installation took place on the virtual machine and all setup and network configuration was done using the provided Sentinel server GUI. There was a minor hiccup during installation – where DHCP was assigning an IP that was already in use for the Sentinel server machine – so we switched to static IP and all setup and network configuration was finished and initial setup was done. We then pointed the software to the license key and were then ready for configuration. The initial setup and configuration of EventSentry in its entirety took less than 30 minutes, allowing us to jump right into testing.

Once installation was complete and the OVF template was properly deployed and configured, we accessed the Sentinel Server through a web GUI. The GUI has an intuitive design that allows for ease of access to all functionality that the product offers. The data collection capabilities are extremely scalable allowing for a variety of deployment strategies: all-in-one, one-tier (two-tier or three-tier) distributed deployment and one-tier distributed deployment with high availability. The all-in-one server deployment designates one system to handle all the log data. The one for two or three tier distributed deployment options allow for data to be scaled out by adding different software components, such as the collector manager, netflow collector manager and correlation engine to other machines in order to offload processing from the central Sentinel Server. Once data events are collected, they are securely transmitted to the Sentinel Server, parsed, normalized, “tagged” and then routed for correlation and archiving. The log archive works extremely efficiently seeing as the files are compressed as a file-based storage. An interesting functionality of Sentinel is its ability to route information to other Sentinel systems, along with correlating data from IPS or IDS systems against known vulnerabilities on the network to provide analysis with collaborative information.

NetIQ provides its customers with either a basic no-cost or a fee-based support option when purchasing the product. Basic offers access to the product knowledge base and support forums on a 24/7 basis. Overall, NetIQ provides more than enough functionality to quickly identify and respond to threats and to simplify management and compliance reporting. This product is a huge step forward for any security team seeking to strengthen security on their network. – JV
SolarWinds Log & Event Manager

SolarWinds includes agents to get detailed logs of different operating systems, hardware, network devices and applications, and includes the ability to parse through syslogs.

Setup involves simply downloading an open virtual appliance (OVA) and deploying it to a hypervisor. After that, we put agents on the machines we wanted to monitor – on Windows, this was pressing the next button, keying in the IP or hostname of the Log & Event Manager, and it just works.

The solution aggregates syslogs, as well as having agents available for many common utilities, such as MS SQL and OSs like Debian or Windows. In many cases, it includes agents that allow for an almost zero setup syslog client. SolarWinds has partners available for a large number of syslog types as well, and we found it could extract useful information from every syslog device in our environment. While most SIEMs allow users to write their own syslog parser, it was nice to see one that had agents for most everything we wanted and included parsers easily available for everything we needed.

SolarWinds makes it easy to look through large numbers of logs with visual, drag-and-drop filters, as well as offering the capability to search. It has a tree map, allowing a user to quickly and easily see things that may stand out in their environment. It also has a word cloud, which is a unique and interesting way to show keywords that appear frequently. Real-time remediation is one of its selling points. On a computer with the agent installed, blocking IPs, disabling networking, force logging off, killing processes and sending messages to the user are all a click away.

File integrity monitoring is quick and easy to set up, and scheduling searches and emailing the results at a time interval are both useful and allow the admin to look for events.

The documentation is some of the best we've seen, available in PDF form with step-by-step examples or, even better, much of it is available through videos, something that can make hard tasks seem easy if done correctly.

As well, the company has one of the best support options we've encountered, 24/7 unlimited phone and email support for the first year included with the product. SolarWinds has an active forum community, large enough to provide support for any potential problems.

SolarWinds is a great value for the money. It is one of the least expensive SIEMs in the market and does not sacrifice quality anywhere in the process. It would be a great product for IT staff on a budget, or a business that involves many endpoints. The only factor that diminishes our assessment of this tool is its lack of unique features.

WatchGuard Firebox M440

The Firebox M440 is the latest next-generation firewall offering from WatchGuard. The M440 is a true enterprise-grade UTM device, with massive throughput and some of the best all-in-one capability in its class. In addition to all of its built-in UTM features, the Firebox M440 can be expanded through licensing to bring to the table advanced malware detection and analysis capabilities as well as DLP functionality.

Out of the box, it comes with tons of built-in templates and a host of other features to make the IT administrator’s job easier.

To kick off our testing, we began by removing the device from its box and installing it in our rack using the supplied hardware. Once we did that, we followed the quick-start guide to create an account on the WatchGuard website to register our device. After retrieving our license, we connected it to our test network and finished setup through a web browser. Here, we configured the WAN interface, set the administrator password and installed our license. All of this was performed through the built-in webpage, which made setup a breeze.

After we finished the initial configuration, we were redirected by the wizard to the device homepage.

We were extremely impressed with the amount of effort that must have gone into the design of the Firebox M440’s interface. After logging in, we were quickly greeted by a heads-up page with all of the goings on in our network. The learning curve for the Firebox was minimal and we found ourselves breezing through the setup of the device for our test bed. We installed a firmware update and then updated all of the web filtering and malware signatures to completely finish integrating the device in our system.

Overall, we were very pleased with the ease of use of the device. Charts, graphs and visualizations are not in short supply on the Firebox, which was another big plus. In addition to its ease of use, we were also pleased with the M440’s performance. Even with all security features enabled, it can still achieve 1.6Gbps throughput, and 10GbE QSFP+ interfaces come standard to facilitate this. An outstanding feature is WatchGuard Dimension, which comes with the purchase. It lets admins view all of the charts, graphs and data from every WatchGuard device enterprise-wide.

Along with the device, we also received a paper quick-start guide in the box. This was well written, included pictures where appropriate and proved helpful throughout the initial setup.

The WatchGuard Firebox M440 is truly an excellent choice for a UTM device. Overall, it is easy to use, expandable and it offers very good value for the price. Its high security and great performance come at a premium price, but it is well worth it. We select this as our Recommended UTM product.

Rating: ★★★★★

SolarWinds

Vendor: SolarWinds
Price: $4,495
Contact: solarwinds.com
Features: ★★★★★
Ease of use: ★★★★★
Performance: ★★★★★
Documentation: ★★★★★
Support: ★★★★★
Value for money: ★★★★★
OVERALL RATING: ★★★★★

Strengths: Price and value for money.
Weaknesses: Lacking in unique features.
Verdict: Great choice for an entry-level enterprise SIEM.

WatchGuard

Vendor: WatchGuard
Price: $6,795 (includes first year of licensing).
Contact: watchguard.com
Features: ★★★★★
Ease of use: ★★★★★
Performance: ★★★★★
Documentation: ★★★★★
Support: ★★★★★
Value for money: ★★★★★
OVERALL RATING: ★★★★★

Strengths: Fast, powerful, 10GbE support.
Weaknesses: None found.
Verdict: Comes from a company with a long history of excellent products. Great bang for the buck. We make this our Recommended UTM product for its power and functionality at an excellent price point.
ZyXEL Communications
USG1900

The ZyXEL Communications USG1900 is a comprehensive UTM firewall that is brilliantly simple to set up. Its small form factor and attractive price point means that organizations of all sizes can set up advanced security quickly and easily. Don’t let its small size fool you though, the USG1900 is teeming with advanced features normally reserved for the largest and most expensive devices on the market.

We started off by removing the device from the box and installing it into our rack with the provided rack ears. After that, following the included diagram, we connected the LAN and WAN network interfaces into our test network. We then connected the power cable and turned it on. We headed over to the USG1900’s web browser interface. Once we navigated to the device’s IP address, we logged in and were redirected to the status page. After this, we opened up the quick setup wizard to configure the WAN interface. Once we finished that, we updated the tool to the latest software version and configured some of its many gateway UTM services.

We were very impressed with the USG1900’s feature set. It is capable of web filtering, gateway anti-virus, application control, SSL inspection and WLAN controller functionality. Even though it is small, we were pleased to see that it is capable of using all eight of the GBE Ethernet ports that adorn its faceplate for a combined aggregate backbone capacity of 32Gbps per second. We were also very happy to see that the USG1900 can perform single sign-on for all of its UTM services. By installing an agent to interface with Active Directory, the USG1900 can see users logging into their computers, then authenticate them and give them the appropriate network access automatically. The ZyXEL tool also comes with built-in templates for many popular business applications.

What’s missing from the picture more often than not are all the products out there that aren’t household names. They have just as many vulnerabilities, but you rarely hear about them, and only if you go looking for the information.

Data just published in the Secunia Vulnerability Review 2015 gives some perspective to what goes on outside of the limelight. In 2014, we recorded 15,455 vulnerabilities, distributed across no less than 3,870 products from 500 different vendors. Of course, not all 15,455 vulnerabilities deserve the same attention as a zero-day flaw in Adobe Flash. Depending on a combination of criticality ratings, market shares and how the individual end-user – private or corporate – is using the vulnerable product in their infrastructure, some vulnerabilities are a bigger threat than others.

The problem with media attention for software vulnerabilities is not that a handful of big names get most of the air time, because they are in use on both private PCs and in corporate infrastructures. This is a good thing as it helps raise awareness around vulnerabilities, mitigation and security in general. It also keeps the right folks on their toes: vendors to issue security patches, and corporate IT teams to patch and mitigate.

What’s missing from the picture more often than not are all the products out there that aren’t household names. They have just as many vulnerabilities, but you rarely hear about them, and only if you go looking for the information.

Data just published in the Secunia Vulnerability Review 2015 gives some perspective to what goes on outside of the limelight. In 2014, we recorded 15,455 vulnerabilities, distributed across no less than 3,870 products from 500 different vendors. Of course, not all 15,455 vulnerabilities deserve the same attention as a zero-day flaw in Adobe Flash. Depending on a combination of criticality ratings, market shares and how the individual end-user – private or corporate – is using the vulnerable product in their infrastructure, some vulnerabilities are a bigger threat than others.

The problem with media attention for software vulnerabilities is not that a handful of big names get most of the air time, because they are in use on both private PCs and in corporate infrastructures. This is a good thing as it helps raise awareness around vulnerabilities, mitigation and security in general. It also keeps the right folks on their toes: vendors to issue security patches, and corporate IT teams to patch and mitigate.

The reality is that some vulnerable products may be in our environment without us realizing it because they came into use in some other context which applications are part of the package when we introduce new products into our environment.

The problem with media attention for software vulnerabilities is not that a handful of big names get most of the air time, because they are in use on both private PCs and in corporate infrastructures. This is a good thing as it helps raise awareness around vulnerabilities, mitigation and security in general. It also keeps the right folks on their toes: vendors to issue security patches, and corporate IT teams to patch and mitigate.

The reality is that some vulnerable products may be in our environment without us realizing it because they came into use in some other context which applications are part of the package when we introduce new products into our environment.

The problem with media attention for software vulnerabilities is not that a handful of big names get most of the air time, because they are in use on both private PCs and in corporate infrastructures. This is a good thing as it helps raise awareness around vulnerabilities, mitigation and security in general. It also keeps the right folks on their toes: vendors to issue security patches, and corporate IT teams to patch and mitigate.

The reality is that some vulnerable products may be in our environment without us realizing it because they came into use in some other context which applications are part of the package when we introduce new products into our environment.

The problem with media attention for software vulnerabilities is not that a handful of big names get most of the air time, because they are in use on both private PCs and in corporate infrastructures. This is a good thing as it helps raise awareness around vulnerabilities, mitigation and security in general. It also keeps the right folks on their toes: vendors to issue security patches, and corporate IT teams to patch and mitigate.

The reality is that some vulnerable products may be in our environment without us realizing it because they came into use in some other context which applications are part of the package when we introduce new products into our environment.

The problem with media attention for software vulnerabilities is not that a handful of big names get most of the air time, because they are in use on both private PCs and in corporate infrastructures. This is a good thing as it helps raise awareness around vulnerabilities, mitigation and security in general. It also keeps the right folks on their toes: vendors to issue security patches, and corporate IT teams to patch and mitigate.

The reality is that some vulnerable products may be in our environment without us realizing it because they came into use in some other context which applications are part of the package when we introduce new products into our environment.

The problem with media attention for software vulnerabilities is not that a handful of big names get most of the air time, because they are in use on both private PCs and in corporate infrastructures. This is a good thing as it helps raise awareness around vulnerabilities, mitigation and security in general. It also keeps the right folks on their toes: vendors to issue security patches, and corporate IT teams to patch and mitigate.

The reality is that some vulnerable products may be in our environment without us realizing it because they came into use in some other context which applications are part of the package when we introduce new products into our environment.

The problem with media attention for software vulnerabilities is not that a handful of big names get most of the air time, because they are in use on both private PCs and in corporate infrastructures. This is a good thing as it helps raise awareness around vulnerabilities, mitigation and security in general. It also keeps the right folks on their toes: vendors to issue security patches, and corporate IT teams to patch and mitigate.

The reality is that some vulnerable products may be in our environment without us realizing it because they came into use in some other context which applications are part of the package when we introduce new products into our environment.

The problem with media attention for software vulnerabilities is not that a handful of big names get most of the air time, because they are in use on both private PCs and in corporate infrastructures. This is a good thing as it helps raise awareness around vulnerabilities, mitigation and security in general. It also keeps the right folks on their toes: vendors to issue security patches, and corporate IT teams to patch and mitigate.

The reality is that some vulnerable products may be in our environment without us realizing it because they came into use in some other context which applications are part of the package when we introduce new products into our environment.
Data exfiltration defense

Knowing yourself is the first step in any operational cybersecurity program. Have a clear understanding of the entirety of your network and internet flows, IP address schemas, ranges, net blocks and architecture. Although exfiltration can happen in almost any form, I’m focusing on mass data exfiltration through internet edges, the mechanism of some of the largest attacks recently.

Generalized edge management and controls are your first concern. I’ve heard the edge is dead, but defining your edge and what traverses it isn’t. Use whatever routing and security technologies you prefer driving bi-directional port and protocol management, leveraging authenticating proxy capabilities, where applicable, and generalized dedicated port management for the remainder.

Once you’ve established a baseline, work with your IT and operations groups to enforce infrastructure assurance processes – like change management/detection and vulnerability management services – to maintain that baseline and record required changes. Rounding out the baseline objectives will be simplistic platform and systems management, like AAA, and forced blogging objectives into centralized monitoring platforms, OS and application patching, and IDM access insurance for data storage.

As you’re geared up to begin deploying advanced detection monitoring capabilities, set yourself up for data exfiltration prevention through anchoring techniques, such as segmentation and funneling. Create network containment techniques to define areas containing the most critical data, use techniques within your information lifecycle and data storage technologies to migrate data to these locations and force the movement of data to/from that environment through specific tunneling routers.

Next, implement technologies, like data leakage prevention, using multiple interrogation techniques beyond simple data matching in a tiered fashion at the host, network and edge. Each layer implemented has a specific control requirement, feature set and policy with an integrated overlapping framework of preventative, detective and defensive control purpose. Through the use of security intelligence and analytics technologies, extend the use of in-place controls through advanced analytics or correlation efforts – all correlated to signify a potential data exfiltration event.

Further, implement inflow decrypt capabilities where legally permissible, handoff to your existing data inspection capabilities and employ application level encryption techniques to extend the most use of the encryption of your critical data across all parts of your stack. Use good encryption hygiene to ensure segregation of duties.

The key to it all is establishing your data exfiltration defense program on top of good fundamental control hygiene and leveraging as much of your existing technology control infrastructure as possible to limit access, protect and monitor the data itself. By doing this, adding in advanced monitoring and focusing on only those business assets necessary to defend, you have a very good chance of advancing your business operations protection data defense capabilities.

Roland Cloutier is global CSO at ADP

A single solution won’t stop data theft, says ADP’s Roland Cloutier.

As practitioners across all industries expand their business operation protection programs in the continuing onslaught of global cyberattacks, a common concern is data exfiltration defense. In today’s complex technology environments, a single process, technology or policy won’t provide an adequate operational preventative capability to prevent exfiltration and identify and respond to negative impact events. A tiered approach of critical network hygiene basics, advanced prevention techniques, better technology and security intelligence capabilities may be the difference between knowing you have a potential issue in time to respond versus finding out too late.

Work with your IT groups to enforce infrastructure assurance processes...
You only have a few WEEKS LEFT!

Register TODAY for SC Congress Toronto

June 10 - 11, 2015
8:15 a.m. - 6:00 p.m.

Metro Toronto Convention Centre

SC Magazine subscribers can register today for $595. At SC Congress Toronto you will:

• Gain insights from leading industry insiders convened only for SC Congress Toronto

• Experience first-hand the latest cybersecurity solutions in our newly enhanced Exhibition Hall

• Network with information security luminaries and peers over two days

• Earn up to 14 CPE credits

Kindly visit our new website at www.sccongress.com and register today. Through April 15, please use Discount Code EARLYBIRDPRINT to receive $700 off the Full Conference Rate of $1,295.

Visit SCMagazine.com for the latest in cybersecurity and to sign up for our newsletters and more.