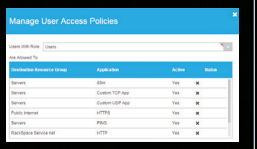
FEBRUARY 2017 • WWW.SCMAGAZINE.COM

SC MAGAZINE
THE CYBERSECURITY SOURCE

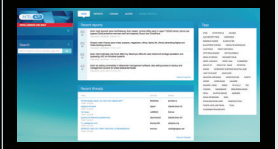
REVIEWED IN OUR GROUP TEST

eSentire P35
Likely to have information that others don't.

FireMon P44
A powerful tool with a clear and important mission.



Intel 471 P48
This tool is the way to monitor the Dark Web.



WHO IS LISTENING?

Your mobile device may be doing more behind the scenes than you think, warns Danny Bradbury. P10

Mobile defense

Companies know that their mobile devices are at risk – and they are taking steps to lock them down. P16

Always connected

What insider threats exist with the use of BYOD mobile devices for work? P20

VOLUME 28 NO. 1 • February 2017 • WEBSITE WWW.SCMAGAZINE.COM • EMAIL SCFEEDBACKUS@HAYMARKETMEDIA.COM

SC MAGAZINE
THE CYBERSECURITY SOURCE

REGULARS

4 Editorial A turning point for cybersecurity?

6 Threat stats A compilation of stats and gauges measuring threat vectors and activity in the world of mobile.

8 From the CSO's desk Dr. Fitband will see you now, by Jon Wilkinson, privacy officer, IBM Watson Health.

9 Letters From the online mailbag.

49 Calendar A guide to upcoming IT security shows, events and courses.

50 Last word Many targets for one email attack, by Ed Jennings, chief operating officer, Mimecast.

Jon Wilkinson P8

Ed Jennings P50

FEATURES

Special focus: Mobile security

10 Hijacking devices: Who is listening?
Your mobile device may be doing more behind the scenes than you know.

16 Mobile defense
Companies know that their mobile devices are at risk – and they are taking steps to lock them down.

20 Always connected comes with risks
What insider threats exist with use of BYOD mobile devices for work? We explore how organizations can mitigate potential risks.

24 Permission denied: Mobile application security
Mobile application security is becoming a tougher battle to wage for organizations, as these apps are demanding more access to users' data.

28 Whatever happened to Apple V. FBI?
SC Media throws it back to February 2016 when Apple and the FBI squared off for a contest that never happened over a controversy that never died.

PRODUCT REVIEWS

32 Product section
We look at open source threat intelligence and cloud-based security management.

33 Emerging products: Open source threat intelligence
Your tools will make a big difference in your productivity and response time.

40 Group Test: Cloud-based security management
As you select a security management system for your cloud/virtual space, the answers are not always straightforward.

46 First Look: EclecticIQ
EclecticIQ Platform is quite likely to add yet another dimension to your analysis.

47 SC Lab Approved: One Year Later
No cyberthreat analyst should be without Silobreaker.

48 SC Lab Approved: One Year Later
Intel 471 is our closed source go-to tool.

SC Magazine™ (ISSN No. 1096-7974) is published six times a year, with combined December/January and July/August issues, by Haymarket Media Inc., 275 7th Avenue, 10th Floor, New York, NY 10001 U.S.A.; phone 646-638-6000; fax 646-638-6110. Periodicals postage paid at New York, NY 10001 and additional mailing offices. POSTMASTER: Send address changes to SC Magazine, P.O. Box 316, Congers, NY 10920-0316. Annual subscription rates: United States: $98; Canada and Mexico: $110; other foreign distribution: $208 (air service). Two-year subscription: United States: $175; Canada and Mexico: $195; other foreign distribution: $375 (air service). Single copy price: United States: $20; Canada, Mexico, other foreign: $30. Website: www.scmagazine.com.

Haymarket Media uses only U.S. printing plants and U.S. paper mills in the production of its magazines, journals and digests which have earned Chain of Custody certification from FSC® (Forest Stewardship Council®), SFI (Sustainable Forestry Initiative) and from PEFC (Programme for the Endorsement of Forest Certification Schemes), all of which are third party certified forest sustainability standards.

haymarket

www.facebook.com/SCMag
www.scmagazine.com/linkedin
www.twitter.com/scmagazine

Editorial

A turning point for cybersecurity?

As we begin another year in the information security industry, I've been mulling how far we've come...as well as how far we still have to go.

We seem at a tipping point of sorts. This last year saw cybersecurity go mainstream in some of the biggest ways to date. Most assuredly it has been a more frequent point of discussion among everyday citizens, politicians and others for some time, but 2016 saw the topic take a wider lead.

PBS specials on it hit, congressional confirmation hearings saw it bandied about like a ping pong ball, the average consumer is increasingly growing distrustful of various companies' data security protections which they do business, and the happenings go on. From presidential debates during which we witnessed a much-maligned and dated stereotypical reference to a "400-pound hacker" to the largest data breaches in history thanks to Yahoo! to predictions that 2017 will see the first nation-state cyberattack acknowledged as an act of war, cybersecurity is facing some interesting times.

Yet, a question remains: Will companies begin taking seriously their information security needs by effectively investing adequate dollars, time, resources and people? Many organizations still are floundering here, of course, but there are those industry pundits who believe 2017 will find a growing number of executives and board members placing more pressure on their CISOs or other cybersecurity leaders to tighten up their organizations' information security plans and solution implementations – an area of focus for this business leaders that they've too often given short shrift.

This view may be quite accurate given some recently reported findings. With the 2016 Ponemon Cost of a Data Breach Study revealing the typical loss for each record pinched by a cybercriminal spiked to $158, a company with millions of records stolen could face serious impacts to revenue streams and some SMEs would close their doors completely.

Requirements to comply with more stringent regulations, such as the EU's General Data Protection Regulation, will find cybersecurity expenditures necessarily jumping. Add crucial needs to shore up security controls associated with expanding cloud-based infrastructures, a widening array of endpoints and newer and impactful technologies like IoT and AI and information-security-related requirements grow even more acute.

Investing in the right solutions and finding the most knowledgeable pros to manage them to effectively underpin business needs will continue to be challenging. However, this tipping point will either see organizations embracing cybersecurity as an enabler and differentiator, which could contribute to their profitability and consumer loyalty and trust, or continue to coast with hopes customer records or intellectual property won't be breached. With many security vendors noting that 2016's cyberattack trends point to a rise in criminals targeting the theft of money-making data, the latter move could tip these companies past the point of no return.

Illena Armstrong is VP, editorial of SC Media.

> "2017 will find executives and board members pressuring CISOs."

ThreatStats

Here's what mobile security looks like.

$3.1T
in annual revenue generated by mobile industry.

Source: App Annie

$3.7T
projected annual revenue by 2020 from mobile industry.

Source: GSMA

3B+
people worldwide now use the internet

Source: Time

35% of communications sent by mobile devices is unencrypted.

87% of time spent using mobile devices is spent using apps.

74% of organizations allow, or plan to allow, employees to use their personal mobile devices for work.

43% of mobile users do not use a passcode, PIN, or pattern lock on their device.

Source: NowSecure

387
new threats every minute, or more than six every second.

Source: IBM Security

In Q3 2016, Kaspersky Lab mobile security products detected:

- **1.5M** malicious installation packages
- **30K** mobile banker trojans (installation packages)
- **37K** mobile ransomware trojans (installation packages)

Source: Kaspersky Lab

60%
of employees access content from outside the office.

64%
of decision-makers read their email via mobile devices.

76%
of organizations plan to invest more in mobile technologies in 2016-2017.

Source: IBM Security

Dr. Fitband will see you now

Jon Wilkinson
privacy officer,
IBM Watson Health

Question: What's the difference between a pacemaker and a fitness tracker app? Answer: Probably about a year or two.

This is neither a clever riddle nor a throwaway happy hour joke; it's an insight into the rapidly converging market of medical devices, mobile applications and consumer wearables.

The pacemaker is a medical device, subject to regulation and approval in the U.S. by the Food and Drug Administration (FDA). If you take an interest in medical device or IOT security (or if you watched the episode of the television show Homeland in which the vice president is killed by a terrorist who hacked his pacemaker), you're likely aware of some of the unique security and privacy risks arising from medical devices that are connected directly to the web or tethered to a smartphone.

The Federal Food, Drug, and Cosmetic Act (FFDCA), which is administered by the FDA defines a medical device in part as, "an instrument, apparatus, implement, machine, contrivance, or implant…which is…intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease." The pacemaker, as a machine used in the treatment of heart disease, clearly meets the definition of a medical device.

So how does a fitness tracker app compare to a pacemaker? Does a fitness tracker app qualify as a medical device?

Currently, the FDA does not consider fitness tracker devices or applications to be medical devices. But two trends are likely to change that in the very near future. First, fitness tracking apps and connected devices are adding features that are increasingly relevant to medical conditions and care, such as SP02 (blood oxygen saturation) or cortisol-level detection. Second, various legislative and financial factors are moving health care toward a model that places more emphasis on preventative care and wellness as opposed to disease treatment. As a result, physicians and other medical personnel are beginning to incorporate fitness tracking devices into treatment plans.

Photo by Andrea Polivy

However, failure to use adequate controls can result in the rejection of an application for a device that has been submitted to the FDA for approval.

The takeaway that applies here goes well beyond medical mobile applications and wearable devices. In the quickly evolving mobile ecosystem, security professionals need to do more than just carefully review current security requirements. Consideration must also be given to trends or possible changes in regulations, enforcement or app and device usage. Long-term product success and your success as a security professional depends on it.

30 seconds on…

»Got device?
The FDA also considers software and applications to be medical devices, when used for diagnosis, cure, mitigation, treatment or prevention of disease.

»Help from apps
There are numerous mobile apps which have received FDA medical device approval, such as diabetes management apps that provide patients with insulin dosing recommendations.

»A world to come
The FDA has issued mobile medical device guidelines, which state in part that, "the intended use of a mobile app determines whether it meets the definition of a device."

»Meeting guidelines
The FDA has increasingly emphasized security controls as a part of the medical device approval process, including security for mobile apps and mobile ecosystems.

Got something to say?

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

From the online mailbag

In response to "Of course it was the Russians," written by Technology Editor Peter Stephenson, an analysis of the JAR report on Russian hacking:

This is an excellent analysis of the report. Probably the best I have seen so far. Many of those using a single data point are using it to point out exactly what you have stated. Forensics is a tricky business and there needs to be much more evidence presented. Intelligence agencies often make best educated guesses. It is sad these government agencies have been so politicized that people no longer trust anything they say.

There has been fairly conclusive proof of other hacking and the government did nothing. Why this, why now? Many feel it smacks of being driven by politics not facts. No one talks about why these targets were so easy to access. There is lots of blame to go around.

I do not doubt that Russians have been actively engaged, it's their motives we are unsure of at this point. The politicians are also making huge leaps with NO data points. There is no proof that anything done had any effect on the election.

Again, thank you for putting all this in perspective and analyzing it in such detail. We can only hope that when the full report comes out our intel agencies have been as thorough and politics have been removed from the entire process. I fear that will not be the case and the real security discussions we need to be having will be lost in the noise.
Todd Hamel

Thank you for your analysis. I, personally, had/have no doubt that the Russians hacked DNC, HRC, RNC, et al. But they are also very "quiet" in that they don't divulge what they obtained. They are in it for information and leverage. Therefore, I doubt that they leaked what they obtained through their hacks.

So, if not the Russians, who has the motive to leak with the goal of embarrassing the DNC and HRC. Well, statistically, a major source of leaks is the employees. Are there angry DNC employees? The answer is 'yes', there are a lot of angry people over the way the DNC treated Bernie and they wanted to hurt HRC and the DNC.

Could it be someone else who leaked the emails? Yes, but as far as the list of possible leakers, I think Russia is at the bottom of the list, and the proof of hacking does not move them up as far as I'm concerned.
Tom Whitmore

In response to a Dec. 30 news article, U.S. sanctions Russia over electoral interference, ejects diplomats:

I read the JAR. Nothing much new there. I'm sure the DNC could use the primer on basic cybersecurity though.
Don Barr

Is the government going to protect my company against retaliation? I don't think so.
Jeannette Anderson

In response to a Dec. 22 news article, EU's privacy statutes preclude U.K.'s data retention legislation, court rules:

U.K., U.S. and Australia have passed laws that invade user privacy and keep eyes on private life of individuals… the more these types of laws are passed the more privacy invasion is done…we citizens need to stop just discriminatory practices.
Robert Emma

In response to a Dec. 9 news article, Obama orders intel probe of election hacks:

These were linked to phishing campaigns, perhaps the DNC and the Democratic Congressional Campaign Committee (DCCC) should invest in some security awareness programs and other common security practices that could help prevent breaches. Blaming the Russians for exploiting your organization through phishing attacks and inadequate security controls is the wrong approach to this problem. The blame falls directly on the leaders of these organizations for not investing in security and end user security awareness programs. With the money that goes through these organizations they should have the same security controls and practices as a multi-billion dollar company.
James McDonald

In response to a news article, Cerber ransomware: Now with database encryption:

Your last sentence forgot "people." Unless they are "endpoints." They're the ones that click on the email link, downloading the ransomware. "Gateway, endpoints, networks, servers and people" is the best multi-layer approach to security.

Great article. DB encryption should be frightening to everyone.
Gregory Hunts

In response to a news story, Cybersecurity unemployment rate at zero:

While the article discusses that they are projecting all these positions. What I find frustrating is those with experience and time seem to encounter difficulties attaining new positions due to companies believing that they can pay entry rates for individuals with 10+ years of experience and the needed certifications that require this amount of time to attain.
Joel Natt

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

MOBILE SECURITY

WHO IS LISTENING?

Your mobile device may be doing more behind the scenes than you think, warns Danny Bradbury.

The next time you open your smartphone, be sure that you know what it's doing behind the scenes. Attackers have been infecting desktop computers for years with malware that enlists them into botnets, hijacking them and placing them under someone else's control. Now, the proliferation of mobile and tablet devices, along with their increasing power, has made them prime targets too.

Tens of millions of devices have been infected and ordered to carry out tasks on the attackers' behalf, undetected by their owners. The era of mobile hijacking is here.

The problem has become increasingly visible to experts recently, explains Dan Waddell, managing director, North America region at (ISC)². "Over the past six years, the category of 'application vulnerabilities' has maintained its position as the top security concern in the (ISC)² Global Information Security Workforce Study, and mobile devices has been in the top five," he says.

"The main thing is to steal credentials," says Solomon Sonya, an assistant professor of computer science at the U.S. Air Force Academy (USAF). Sonya, who has also been an officer in charge at the Air Force Computer Emergency Response Team (AFCERT), presents on mobile security and authored a proof of concept mobile botnet client called Splinter in 2012.

Just as with regular botnets, stealing credentials is a common tactic for malicious applications that hijack smartphones, he says. "So many users will still check their bank accounts on their phones, log into Facebook, and log into their email, which is just as juicy as a bank account." The reason: an attacker with email access can reset passwords for countless online services.

Mobile application hijacking shares another common payload with traditional desktop botnets: advertising fraud. Online advertisers pay people displaying their ads when visitors click on them, but they often don't distinguish between legitimate and illegitimate publishers. Malicious applications will digitally simulate users without their knowledge, artificially "clicking" online advertisements, using up computing resources and bandwidth on the victim's phone to earn money for the malware authors.

"The actors behind these malicious advertising families are well funded, and have their own internal app development teams that are dedicated to creating unique applications to lure users into installing their applications," says Andrew Blaich, security researcher at Lookout, which sells mobile endpoint security tools.

A report on ad-serving apps from anti-ad fraud firm Forensiq revealed that these ads will often call online ads as often as 20 times per minute, compared to legitimate apps that call new ads twice a minute at most. They will also access affiliate links to generate revenue for the attackers from those sources.

Some malware also hijacks other legitimate applications running concurrently on the device to show its own ads. For example, NoIcon, a

component of the YiSpecter malware found on iOS devices, detects apps running on a device and then uses another malware component, called ADPage, to show full-page ads for its authors.

Gooligan, a form of malware embedded in Android apps downloaded from third-party app stores, focuses on mobile app advertisements. After obtaining root access to the phone it simulates user clicks on advertisements for legitimate apps, and then uses Google Play store account credentials stolen from the phone to install them. The attackers then gets a fee from the unwitting ad network.

Ad fraud using malicious apps is endemic. Forensiq's report analyzed 5,000 apps flagged for ad fraud over 10 days and found more than 12 million unique devices running at least one of these apps. That puts them on around one percent of all the phones in the U.S. and two to three percent of those in Europe and Asia.

In the back

These malicious applications will typically run as a background process on the phone, booting at startup, which makes them difficult to detect. They can be installed in various ways. Sideloading – installing tempting applications from unapproved third-party app stores – is one method. Deliberately jailbreaking or "rooting" phones to install ad hoc, unapproved applications – is another. Both are inadvisable.

> "The main thing is to steal credentials."
>
> – Solomon Sonya, U.S. Air Force Academy

Even applications that have been scanned and approved by Google or Apple can be dangerous, though. Sonya recalls the Android/Mapin trojan embedded in many games. "It would wait between one and three days before the malicious payload would execute on the machine," he says. That makes it hard for automated scanners to spot.

Another approach is simply to compromise the software tools used by a legitimate developer, turning them into your unwitting pawn. That's what happened with XcodeGhost, a malware attack that hit dozens of applications in 2015.

"XcodeGhost embedded itself in the integrated development environment for writing Apple's products," Sonya recalls. Attackers released a version of the Xcode IDE on Chinese forums, promising faster downloads than Apple's official version, but it added malicious code when they compiled their iOS applications for submission to Apple.

"Many applications were compromised with additional code injected into it from XCode Ghost," he continues. At the time, experts worried that hundreds of millions may have downloaded the compromised apps, which included regional versions of WeChat and Angry Birds 2.

Others have attacked Apple devices by using an enterprise developer account, which provides digital certificates intended to distribute in-house applications. Some attackers (such as the developers of YiSpecter) have misused these certificates to distribute malware more widely. It also enabled them to use otherwise-unavailable private application programmable interfaces (APIs) in iOS to perform more sensitive operations, such as masking their programs.

There have been several examples of malicious mobile apps circumventing Apple and Google's scanners to hijack innocent users. Apple's scanning system overlooked AceDeceiver, a family of malware apps, seven times, according to researchers at Palo Alto Networks.

Attackers then capture the authenti-

HARD CELL: Stingray

Malicious apps aren't the only things that are eavesdropping on mobile data these days. Cell site simulators, otherwise known as IMSI catchers, are hardware devices that fool cellphones into divulging their secrets.

Cell site simulators conduct a man in the middle (MITM) attack on a cellphone by impersonating a cell tower.

"In doing so it has access to all of the data your phone sends or receives in plaintext, and often much of the encrypted traffic," says Rob Wood, principal consultant at NCC Group, a global cybersecurity and risk mitigation provider. "The controversy is that these devices are not always selective in which devices they affect, so are classified as mass-surveillance."

IMSI catchers can triangulate the location of phones in the area, but may well be able to listen in on text messages and other communications from phones that connect to them, due to the way that modern communication systems work. Encryption only exists between the phone and the cell tower, which can often dictate the type of encryption used during the session, if any. The NSA has demonstrated the ability to decrypt certain cellular encryption protocols.

The Stingray the common brand name for IMSI catchers, is produced by U.S.-based Harris Corp. and has been used by the FBI since at least the mid-90s. Local law enforcement in many states also use the devices. So secretive is the use of this technology that the FBI has moved to dismiss cases in which details of the technology may be exposed. However, reports suggest that IMSI catchers can be built by anybody with a moderate degree of technical expertise.

cation codes provided by Apple when installing these apps and provide them to a malicious PC client that pretends to be Apple's iTunes software. The software then uses the codes to install the apps without the user's knowledge on iOS devices connected to computers running that software.

The ramifications of mobile hijacking can be dramatic for different stakeholders. Ad fraud is a drain on the advertising industry, according to the Internet Advertising Bureau, which researched the issue in conjunction with EY. It found that invalid traffic is costing the U.S. online advertising industry $4.4 billion per year – more than its combined revenue losses from ad blocking and pirated content.


Tammy Moskites, CIO & CISO, Venafi

Aside from the direct security implications of stolen credentials, users also suffer from ad fraud because of the computing and bandwidth resources used up by the secretive ad-clicking used by the apps. Forensiq estimates that a typical malicious app can use up to 2Gb of data per day, chewing up data plans and battery life.

> "For extremely sensitive data, we're moving to a VDI model..."
>
> – Mark Walton, South Western Utah University

Protection?

How can CISOs protect their users – and their organizations – from mobile hijacking? The bring-your-own-device (BYOD) trend has blurred the lines between individual and organization, points out Sonya, making consumers a threat vector for their organizations.

"The person is the main focus because they're easier to fool," he says. "People love to download those free games and apps. Once you're on that network I would spread out."

This is precisely what Dresscode, a malware strain found in hundreds of certified Google Play store apps, has been doing. The malware links an infected Android phone into a botnet that can be directed to click on ads. It also allows attackers to control the phone while connected to a corporate network and download files, a study from Check Point reported.

"CISOs are aware of this problem but they are always trying to balance employee and business productivity against security," points out Tammy Moskites, CIO & CISO at Venafi, and former CISO at Time Warner Cable.

"In most cases, organizations have decided that the security risks associated with BYOD are outweighed by the productivity benefits for employees so they are looking for other ways to mitigate the security risks," she adds.

What are those other measures? Installing anti-virus software onto mobile devices can't hurt, but don't rely on it. "While AV software can detect some of these rogue apps, it is consistent with our research that the majority go undetected by such software," says John Douglas, director of product strategy at Sizmek, which sells products to help companies create and manage online advertising campaigns. "AV providers also need to make ad fraud detection more of a priority in their own business models."

Other evidence shows that mobile AV is an art rather than a science. Palo Alto Networks found that of 57 security vendors in VirusTotal, only one detected YiSpecter after 10 months in the wild.

Sonya agrees that AV isn't enough. He only began noticing anti-virus tools detecting the first version of his Splinter botnet in 2015 – three years after he wrote it as a proof of concept and uploaded to VirusTotal.

In any case, trying to control security on mobile devices that you don't own is a fool's errand, suggests Rob Labbé, director of information security at a major mining company in Canada.

"Make sure the secure decisions are made in a place you can control," says Labbé, who proudly highlights his use of mobile data management as a management rather than a security tool.

"It's a security design mistake to have security decisions made on the client," he says, adding that the trick is to assume these devices are already compromised. "One can argue that it's a bigger mistake when that client's on mobile, but it was a stupid idea to begin with."

Mark Walton, director of IT security, South Western Utah University, stays equally paranoid about unknown devices. "Any non-IT issued device is untrusted, and thus is limited as to what kinds of information it can access," he says. "For extremely sensitive data, we're moving to a VDI model where we have more control over the environment, and have policies concerning where sensitive data can be accessed and stored."

As mobile devices look increasingly like computers, we're headed to a world where people spend more time using them for business and personal purposes than they do using desktop operating systems. Mobile hijacking is now a mainstream trend – and it shows no sign of stopping. ■

A more extensive version of this article is available on our website.

MOBILE DEFENSE

Companies know that their mobile devices are at risk – and they are taking steps to lock them down, reports Steve Zurier.

The threats from mobile malware have been highly documented:

Zimperium reported late last year that 60 percent of mobile devices in enterprise BYOD environments are vulnerable to known cyberthreats. About six percent surveyed recorded a critical threat event and one percent were infected with a malicious application.

And Skycure reported that 32.5 percent of devices used by executive were exposed to network attacks in the April through June 2016 timeframe. Over that same period, 22.5 percent were infected with malware that rated at least a medium severity of risk and 6.3 percent were determined to be a high severity risk.

In fact, it was this increased threat landscape and other major events in the mobile malware world, such as the Pegasus malware that infected iOS devices and the Stagefright bug that hit Android smartphones and tablets, that prompted global mining company Kinross Gold to get more serious about protecting mobile devices.

"We were using AirWatch for mobile device management, but we needed something that could detect and remediate mobile malware," says JT Pearson, manager of IT client services at Kinross Gold Corp. "When I think back, it was really the Sony case that cemented security in the minds our corporate board, and this was after we had highlighted the need for mobile security in many previous conversations."

Kinross employees were originally BlackBerry users, but as the Canadian-based gold mining company moved its company-owned devices to Android and iOS, it needed a way to save on phone charges. Pearson says the company has mines and projects in Brazil, Chile, Ghana, Mauritania, Russia and the Unites States and it was spending excessive amounts on roaming data when its executives traveled abroad. For example, simply checking email often resulted in a $200 charge in a single day, Pearson explains.

He adds that while Wandera was originally viewed as a cost-savings tool, it became even more important to the company when the

OUR EXPERTS: Road warriors

Edward Amoroso, CEO, TAG Cyber
Brian Heemsoth, director of software and mobile security, Aetna
Patrick Hevesi, research director, Gartner
JT Pearson, manager of IT client services, Kinross Gold Corp.

vendor added new security features and was then seen as a way to more effectively respond to the emerging threat landscape.

Now, data and content travels through Wandera's cloud-based system that compresses the data and inspects it for malware, a process that significantly reduces data use. Kinross Gold also takes advantage of some of its other security features. For example, Pearson says Kinross Gold enables hard blocks on software updates as well as caps on data usage when employees are roaming.

"If you hit 200 megabytes on any given day we'll stop you," says Pearson. "We also block optional apps, such as Instagram, Spotify and some streaming services while roaming."

Pearson adds that by using Wandera's compression, blocking and active management capabilities, Kinross Gold saves roughly $750,000 on its annual cellular bill for the 250 employees who have company-owned devices.

> "If you hit 200 megabytes on any given day we'll stop you..."
>
> – JT Pearson, Kinross Gold Corp.

A more strategic approach

"We explained to the board that we had seen an increase in both phishing emails and attacks by macro-embedded malware in mobile devices," Pearson says. "So when we explained that we could deliver enhanced security and also save the company significant money on its annual data use charges it just became a much easier sell."

Patrick Hevesi, a research director on the security and risk management team at Gartner, says while tools such as enterprise mobility management (EMM) can help companies manage and update phones and mobile threat defense, and mobile threat defense (MTD) products can ward off network attacks and malicious applications, companies also need to be more strategic about how they manage mobile devices.

JT Pearson, manager of IT client services, Kinross Gold Corp.

Hevesi says he starts by telling IT staffs to keep updates consistent. Companies also need to assess risk and decide what level of access each person's phone will have. Of course, there may always be some data and intellectual property that are so sensitive they may never be put on a mobile device, but that's not the vast majority of a company's applications.

For example, Hevesi says employees who need access to sensitive company data and require a higher level of security should always get company-issued phones that have EMM and MTD agents installed. Employees who are just doing standard business applications and checking emails can use their own personal devices, but they have to let the company at least put an EMM agent on the phone and MTD on a case-by-case basis. For lower-level employees who may be only checking email, it makes sense to install an MTD tool to protect against mobile malware.

"For most people, if you give them a choice and explain why you are putting on the added controls, they will work with the company," Hevesi says. "The idea is to not make it a battle."

Health insurance company Aetna has a very clear approach based on access to sensitive data it developed to manage nearly 10,000 mobile devices, a mix of iPhones, iPads and Android smartphones and tablets.

Let's get personal

Brian Heemsoth, director of software and mobile security at Aetna, says employees who handle sensitive information such as personaly identfiable information (PII), medical, or credit card data receive company-issued devices that are managed by a mobile device management (MDM) platform such as MobileIron, AirWatch or IBM's Maas360. The majority of the staff – roughly 60 percent – use standard productivity tools and email, so they can run their personal iPhones or Android devices.

MOBILE DEFENSE: Terms

Enterprise mobility management (EMM) – people, processes and technology focused on managing the increasing array of mobile devices, wireless networks, and related services to enable broad use of mobile computing in a business context.

Mobile device management (MDM) – the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers.

Mobile threat defense (MTD) – his rise in the sophistication and volume of mobile malware and continued exposure to unknown vulnerabilities demonstrates how Android and iOS devices simply aren't secure on their own.

Source: Wiki/Gartner

Heemsoth says as mobility has become more of a fact of life in corporate America, a number of trends have converged in the past few years that made his firm focus more on mobile security. First, more people travel for business today, so there's been an explosion in mobile collaborative applications. Second, people want to work on just one phone, not on a company-issued BlackBerry in addition to their own personal phone. And finally, the threat landscape for mobile malware has become more hostile than ever.

"There's been a growing trend toward people wanting to use just one device to handle both their personal and corporate communications, and we want to accommodate that," he says. "We also want to let people use the iPads that they received as gifts over the holidays, but there has to be a way to keep everything secure."

> "That visibility into our mobile risk is what's key."
>
> – Brian Heemsoth, Aetna

Brian Heemsoth, director of software and mobile security, Aetna

About a year ago, Aetna deployed Skycure's mobile threat defense application on all 10,000 of its phones. Skycure checks for malware and also will automatically reroute an employee who logs on to an insecure network via a secure VPN tunnel. The VPN tunnel acts as a secure gateway to the internet.

"Since we launched a year ago, we've seen a self-remediation rate that averages about 18 per user," Heemsoth says. "People can easily take action in response to guidance to update their operating systems or remove third-party applications that may contain malware."

The right stuff

Heemsoth adds that for company-issued devices, they've tightly integrated Skycure's mobile threat defense with MDM/EMM software, the employee and the company's security operations center.

Here's the way the integration works: When Skycure identifies malicious code, it notifies the MDM/EMM system, which then severs access to all the secure networked applications. Skycure also alerts the employee that this took place and will also send an alert to the security operations center (SOC), which will prompt the incident response team to remediate the malware.

Heemsoth advises security managers to realize that integrating best-of-breed products makes sense, but it also takes the right people who know how to work with all these tools. He acknowledges that Aetna is a Fortune 50 company with the resources to spend on top quality tools and talent. More mid-tier companies may require a systems integrator to deliver a similar capability. Heemsoth adds that tight integration into all the security tools offers the company visibility into the threat landscape that they never had before.

"That visibility into our mobile risk is what's key," he says. "We now carry fewer vulnerabilities, experience fewer malware infections, and the proactive network security protection has been huge, especially for our workers on the road." ■

MOBILE: Three trends for 2017

Edward Amoroso, CEO of cybersecurity consulting firm TAG Cyber, and former SVP and CSO of AT&T, offers three mobile security trends to look out for in the upcoming year:

Malware will move to voice. The audio conversations of some high-profile officials will wind up on WikiLeaks sometime this year. In his view, there's no logical difference between voice and data anymore, so it makes sense that voice conversations will be the next attack vector. Security teams might be smart to consider some sort of over-the-top encryption for their mobile devices.

Expect even more serious malicious applications to proliferate. Applications such as Pegasus and Stagefright were just the beginning. Security teams will be increasingly challenged in 2017 by malware that can be jailbreaked remotely. This will require additional user awareness training on how to be more careful about clicking on potentially infected URLs with mobile devices.

Vendors are responding. On a more positive note, there are better tools now for CISOs to deploy – and they will keep improving in 2017. Leading MDM companies – such as Mobile Iron, AirWatch and IBM Maas360 – are now almost entirely security-focused. And MTD products – from the likes of Better Mobile, Check Point, Lookout, Skycure and Zimperium – can be integrated with analytics systems, such as Splunk, so security teams can detect, remediate and generate reports about the ongoing threat landscape. While nothing is foolproof, better tools will make managing a difficult threat landscape somewhat easier.

ALWAYS CONNECTED COMES WITH RISKS

What insider threats exist with use of BYOD mobile devices for work? Larry Jaffee explains how organizations can mitigate potential risks.

As Hillary Clinton learned all too well, you can't be too careful protecting sensitive material, and co-mingling work and personal email on various devices is never a good idea.

WikiLeaks and the outcome of the 2016 presidential election notwithstanding, it behooves all organizations to better examine just how vulnerable their networks are when non-company-issued mobile phones and other devices are able to access proprietary records.

Make no mistake, criminal elements are banking on the gaping sieves created when employees connect to the internet via public Wi-Fi and charging stations.

As the Ponemon Institute noted in January 2016, security issues – think about the rampant deluge of serious breaches since then – will not curb the use of mobile devices and their access to and storage of sensitive data. Among the 720 Ponemon survey respondents in the U.S. using smartphones and tablets for personal matters and/or business, 59 percent access corporate email and documents from those devices.

About two-thirds admit that the amount of sensitive/confidential data on devices increased significantly during the previous two years. Further, a March 2014 Ponemon survey conducted by IBM found that 63 percent of the 618 IT and IT security practitioners surveyed believed data breaches involving mobile devices occurred in their organizations.

Gorav Arora, director of technology for data protection, Gemalto

Yet lackadaisical attitudes remain in ensuring everything is being done to protect assets from being inadvertently siphoned from employers' physical confines, SC's panel of experts concur.

To what extent organizations implement stringent policies regarding bring-your-own-device (BYOD) runs the gamut, according to Kevin Haley, director of security response at Symantec, a Mountain View, Calif.-based technology company.

"We're seeing everything from stringent policies in place to no policies at all," he says, adding that in some cases, tools have been put in place for enforcement, whereas in others they have not.

Stolen or lost devices should be treated as a breach because "mobile devices ultimately become a way for insiders to take data outside of an organization," Haley notes.

One of the biggest threats businesses face with work usage of mobile devices is the misalignment of the security practices with risk tolerance, points out Gorav Arora, director of technology for data protection at Gemalto, an Amsterdam-based digital security company.

"It can take the form of unintentional misconfiguration of a new tool due to the lack of knowledge, or could be intentional circumvention of security policies by employees to achieve higher productivity, meet deadlines, etc. – such as emailing sensitive information over personal email for a colleague who cannot connect to VPN," Arora says.

The rise in the adoption of "shadow IT," which is the abandonment of corporate security policy, is a direct indicator of the gap between the provided IT tools and needs of the employees, Arora believes.

Furthermore, once a device is out

OUR EXPERTS: BYOD

Gorav Arora, director of technology/data protection, Gemalto
Rick Caccia, CMO, Exabeam
Ken Dort, partner/chair IP Group, Drinker Biddle
Keith Graham, CTO, SecureAuth
Kevin Haley, director, security response, Symantec
John Michelsen, chief product officer, Zimperium
Sean Sullivan, security adviser, F-Secure

of the company or an employee's possession, it's typically mined for credentials, company data and personal information, points out John Michelsen, chief product officer at Zimperium, a San Francisco-based mobile security company which recently collected data from 7,000 mobile devices used by a client's employees. It found 60 percent of the devices to be exposed to known vulnerabilities, six percent recorded a critical threat event and one percent to be infected with a malicious app. (Adding to those findings, Symantec's "Internet Security Report," identified a 77 percent increase in Android malware variants from 2014 to 2015, with even more expected in 2016.)

"This 24/7 access, outside the corporate firewall, likely raises the tendency of employees to share inappropriate information with others," Michelsen says. Organizations should implement solutions from mobile device manufacturers that provide strong authentication, document tracking/tracing and data loss prevention features, he adds.

> "Mobile doesn't create new types of insider threats."
>
> – Rick Caccia, CMO, Exabeam

Keith Graham, CTO, SecureAuth

Sean Sullivan, security adviser, F-Secure

Authentication required

As BYOD became prevalent, device manufacturers are turning on security by default, essentially building in two-factor authentication to secure company data, notes Arora at Gemalto. Only two-fifths of enterprises use authentication to protect all of their resources, but it should be a standard business practice, he adds.

Organizations should ensure that if applications are being accessed from mobile devices, suitable authentication safeguards are being used such as ensuring that adaptive authentication and second-factor methods are in place, agrees Keith Graham, CTO at SecureAuth, an Irvine, Calif.-based provider of two-factor authentication and single sign-on tools.

If a device is compromised and any credentials being used on the device are stolen, adaptive and second-factor authentication "helps ensure that attackers cannot use these stolen usernames and passwords to gain access," he adds.

Paying attention to what's going on in the network is critical whether the employee is in the office or working remotely. "Log analytics, particularly those that use behavioral analytics, can identify risky access patterns early in the process," says Rick Caccia, CMO of Exabeam, a San Mateo, Calif.-based computer security services firm whose specialty is behavior analytics.

Caccia believes that putting more security on the device itself has only marginal benefit. "It's much better to increase monitoring and detection throughout the network itself, and then to link that to cloud services in use," he explains. That way, even if an employee switches devices, the firm can detect unusual behavior.

The mobile arena, because of less device management, "can make it easier for a malicious insider to copy and remove sensitive information," he points out. "Mobile doesn't create new types of insider threats, it just makes the most common types easier to execute and harder to detect."

Part of the problem is an office desktop computer and server mentality is influencing IT departments without acknowledging workflows have changed dramatically. By their very nature, mobile phones are reliant on non-desktop technologies.

"We've seen numerous cases of attacks orchestrated where a one-time-password sent to a phone via SMS has been intercepted and stolen from the mobile device using malware," Graham notes. This, of course, enables attackers – with already compromised usernames and passwords – to bypass the second factor.

Meanwhile, Haley points out that mobile phones are "great spying tools" that can take pictures and record audio and video, and even report the location to an insider who could control the device.

A social engineering ploy that tricks an employee to click on an emailed, malware-infested link accessed from a BYOD can easily result in a data loss, or worse.

"Business email compromise (BEC) exploits the hyper connectivity and mobility of the workforce," Arora notes. "Often such threats start with phishing attacks to have unwitting trusted insiders allow privileged access to untrusted outsiders, leading to the installation of malware or ransomware," he says. In June the FBI estimated such attacks have resulted in $3 billion being swindled from businesses around the world, he adds.

Back to basics

Organizations need to go back to basics. "There is no substitute for continuous security training and education of all employees to ensure the security mindset permeates through every business transaction and is weaved into company culture," Arora points out.

To mitigate risk, organizations need to shift their mindset toward "breach acceptance" rather than prevention, he believes.

Although mobile devices allow the unification of multiple accounts, many users end up using personal accounts for work. "Not good," notes Sean Sullivan, security adviser for F-Secure, a cybersecurity and privacy company based in Helsinki, Finland. "There should be a clear division between personal and professional accounts," he says.

He also urges employees to learn how to archive. "There is almost no good reason to keep 10 years of communications at your fingertips," he says. A desktop client can sync a mailbox and archive the old stuff to an offline file. "Then delete and sync. If you don't know how, get an IT staffer to assist."

> "There is no substitute for continuous security training..."
>
> – Gorav Arora, director of technology, Gemalto

Not taking all the precautions in protecting health and financial data, for example, opens an organization to legal liabilities. Ken Dort, a partner in the IP Group of Chicago law firm Drinker Biddle and chairman of the firm's Technology Committee, notes that companies have regulatory responsibilities in safeguarding personally identifiable information (PII) relating to employees or customers, and personal health information of patients held by health care providers.

Proprietary and/or confidential information – such as research and development plans, corporate financial data, marketing plans and pricing information – can be valuable to competitors.

"The ubiquitous use of mobile devices to permit the flexibility of today's workforce has exposed sensitive data to greater risk of loss as these devices leave the secure facilities or systems of companies with otherwise solid security practices," Dort says.

The fact is mobile data faces a higher risk of loss than data kept within the walls of a company's secure framework. "Given the small size of most mobile devices, intentional theft of data by disloyal insiders becomes easier as the capacity of these devices grows ever larger," he adds.

Arora notes that the data perimeter has been eroded by the mobile workforce and adoption of the cloud. Focus should instead be on securing the data through encryption and strict access controls, and using strong authentication to elevate the assurance of the end-user identity, he says. ■

MINIMIZE THREATS: Four must-haves

How can organizations reduce and mitigate the mobile threat posed by its own employees? Kevin Haley, director, security response at Symantec, lays out four simple must-haves that organizations should implement to reduce and mitigate the threat:

1. **Policies**: Have policies about the use of data and ensure users are educated on them
2. **Tools**: Use tools to both alert and prevent data leakage
3. **Encryption**: Leverage encryption on mobile devices to protect data
4. **Scanning**: Ensure devices are scanned for spyware and malware

Haley also suggests any mobile toolkit should include protections such as two-factor authentication, data leak prevention, and encryption/remote wipe technology.

PERMISSION DENIED?

Mobile application security is a tough battle to wage since apps are demanding more access to user data, reports Karen Epper Hoffman.

Just as they did on the desktop, applications on mobile devices are becoming more prevalent, more useful and more necessary to making the smartphones and tablets the go-to workhorses for an increasing number of corporate employees.

But as these applications get better and more pervasive, they are also becoming more of threat vector for attacks – not only because of their ubiquity, but because of the sensitive information they hold. According to an HPE study, "Mobile Application Security Report 2016," the potential threat to privacy and reputation is very real from applications that often collect unnecessary data. In 2015's Ashley Madison breach, for example, the company's storage of geolocation data allowed a reporter to pinpoint the location of otherwise anonymous users.

"Mobile applications have had a steady rise in risk for companies, and that's mainly due to the shift from desktop browsing to mobile applications," says Ryan O'Leary, vice president of the Threat Research Center and technical support for WhiteHat Security, a Santa Clara, Calif.-based web application security firm. "More and more of the everyday online tasks people do are being shifted to mobile application. As more people move to mobile applications to conduct transactions, the greater the risk is to the companies that deploy these."

In addition, O'Leary points out that mobile applications are native apps, meaning they're downloaded and run on the phone. If a security issue is found, the company often must make changes to the application code. "This requires users to update their application or it will continue to be vulnerable," he adds. "It is in the hands of the user to remember to update applications regularly."

Michael Taylor, applications and product development lead for Rook Security, a computer security services firm based in Indianapolis, agrees that mobile applications have become a more attractive target in the past year due to their ubiquity, their increased utility and their advancing system capabilities (including RAM, CPU and storage). As a result, he says that the increasing size of the mobile app ecosystem has caused its own series of problems. "Many apps with vulnerabilities, excessive device access requirements and malicious updates have been released that can expose the end-user to remote access tools, remote monitoring and data exfiltration," he says.

Indeed, Gregory Leonard, senior application security consultant for Optiv, an information security company based in Denver, points to the sheer number of mobile applications combined with the growing prevalence of the bring-your-own-device (BYOD) movement making mobile applications a more appealing target. "IT network security teams are challenged by the mobile space because IT policy cannot completely control

access to a mobile device like they could with desktop or laptop computers," Leonard says. As an example, he points to the Stagefright bug, which enables attackers to send a specially crafted MMS to a device and perform remote code execution and privilege escalation, typically without requiring any user actions.

But perhaps the most pernicious issue is that of how more mobile applications demand a high degree of access and control over a user's system and their data in order to even be downloaded. "A key issue here is that most are not aware of the sheer amount of information captured by mobile applications, such as contacts, calendars, geolocations, photos, attachments and more," says Brian Stafford, CEO of Diligent, a New York-based firm that provides secure collaboration for boards and leadership teams. "This needs to change."

Stephen Gates, chief research intelligence analyst for NSFOCUS, a Santa Clara, Calif.-based provider of enterprise-level network security solutions and services, agrees that the demand for permissions employed by most mobile applications has gotten out of control. "You start looking at the permissions required by an application on the Google Play store and it wants to look at your contacts, location, modify or delete the contents of your SIM card… Why in the world would any application need to have all this access?" he asks.

And, with so many mobile users unblinkingly agreeing to give mobile apps this broad access, a new door

> "IT network security teams are challenged by the mobile space..."
>
> – Gregory Leonard, Optiv

has opened wider to the emergence of "imposter applications," created by hackers to spoof legitimate and popular mobile applications to gain a foothold through mobile devices. John Michelsen, chief product officer at Zimperium, a San Francisco-based company that offers enterprise-class protection for mobile devices, says that initially, when Pokemon Go was only available in a few countries, users began going to third-party app stores to download the popular game application. "Hackers caught wind of this and created imposter apps loaded with spyware, remote access trojans and bots that gave cybercriminals complete control over users' mobile devices," Michelsen says, adding that more imposter apps duped shoppers at Foot Locker, Dillard's, Nordstrom and Christian Dior this past holiday season.

Brian Stafford, CEO, Diligent

Securing mobile apps

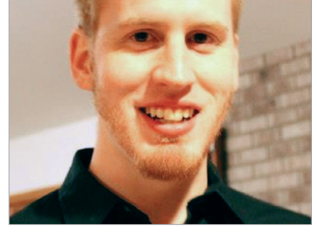
WhiteHat Security's O'Leary points out that even company-issued mobile devices can have inherent security risks depending on how they are deployed. "Users are much less likely to care about the security of their work phone than that of their personal phone," he says. He suggests that a mobile user is more apt to set up their personal phone with better passwords, lock screens that require authentication to unlock, and employ the use of two-factor authentication. On the other hand, O'Leary says, many mobile users see a work phone as something one has to have, so users often ignore basic security practices. "And users are often reluctant to have anything installed on their personal phone that mandates security, or is seen as a 'big brother' practice. It's then up to the user to make sure they're following good security practices."

But with BYOD becoming more widely embraced in all sectors – as a means of reducing costs and demands on IT – mobile application management and security become trickier. "Employees don't expect personal privacy when operating a company-owned computer, so surveillance-style security solutions meet little resistance from users," Zimperium's Michelsen says. "But when employees bring their own mobile devices to work, monitoring web searches, messaging content and other application activity becomes a major violation of privacy." Hence, he says enterprises cannot duplicate their existing endpoint security processes for mobile.

The major issue here is that most companies implement BYOD policies without having compliant and secure programs in place for all of their employees and members of the organization, says Stafford of Diligent. "It is the responsibility of the business to make sure they are aware of the applications their employees are using in order to come up with a security solution and procedure in advance."

John Labelle, senior security consultant at Optiv, believes that much as they do with web applications, "organizations should assume that the client side of mobile applications is not completely secure. Attackers will always be able to look into and alter functionality, even for binaries or obfuscated code." Leonard, also at Optiv, points out that another hurdle with mobile application security is that "it takes time to deliver security fixes to devices." Some manufacturers do a good job of providing regular updates to a majority of their devices, while others have to deal with a much more complicated delivery process, where an update to a device has to wait on security patch development from the operating system development team, the device manufacturer and the specific cellular carrier on which the device is running, Leonard adds.

"Also, mobile applications can be easily downloaded and reverse engineered by attackers, giving them a better understanding of how an app works and how it possibly can be exploited," Leonard adds. "This gives them a significant advantage over a traditional web application, where the application code is stored on a server which would need to be compromised before the application could be inspected."



John Labelle, senior security consultant, Optiv

Gregory Leonard, senior application security consultant, Optiv

Outsourcing to third parties

An added complication is that mobile applications are often outsourced to third-party developers who have

> "These apps could have serious vulnerabilities..."
>
> – Ryan O'Leary, WhiteHat Security

expertise in mobile application development, O'Leary points out. "These third-party developers often care more about getting it done quickly than building good security practices in," he adds. "We've seen some pretty egregious vulnerabilities in recent mobile applications." For instance, O'Leary says one mobile application asked for an email and password to register; if the email already existed as a user, it would simply update that user with the new password. "Effectively, I could update anyone's password and login as them if I knew their email," he adds.

When an organization is developing its own mobile applications, they should follow a secure development lifecycle with all the normal steps of threat modeling, security architecture, security testing, training and the rest, says Jeff Williams, co-founder and chief technology officer of Contrast Security, a Los Altos, Calif.-based application security firm. He adds that internal developers should consider the OWASP Mobile Security Top Ten project as a good starting point for specific risks. And when it comes to externally developed mobile applications, Williams says companies should be very careful to select those that have a strong security story about how their code is built, secured and tested. "They should use mobile device management (MDM) and mobile application management (MAM) solutions to control risks to their enterprise from those applications."

For his part, O'Leary believes more compw that would completely devastate a company," he adds. "Getting a good third-party security assessment on your mobile applications is a must." O'Leary also suggests that organizations have a specific plan in place to fix these mobile vulnerabilities as soon as they are detected. "Once it's released and a vulnerability is found, your user base is vulnerable until all of them update their application," he points out.

But even when it comes to established security approaches, it seems harder to strike a balance between making users safer and making it harder for them to manage their own applications. Optiv's Labelle is seeing more companies use anti-jailbreaking trapping and source obfuscation tools. "This isn't going to have the desired effect, which is improved security," he says. "Making an application harder to use or understand does not always make it more secure." People who may want to help – consultants or researchers, for example – can be locked out of the process of improving security if the application becomes too unwieldy for anyone but those familiar with it, he says.

"Basically, when you raise the bar so much that good guys can't access your app, the only ones left looking are the bad guys," Labelle adds. ■

OUR EXPERTS: Mobile security

Stephen Gates, chief research intelligence analyst, NSFOCUS
John Labelle, senior security consultant, Optiv
Gregory Leonard, application security consultant, Optiv
John Michelsen, chief product officer, Zimperium
Ryan O'Leary, vice president of the Threat Research Center, WhiteHat Security
Brian Stanford, CEO, Diligent
Michael Taylor, applications and product development lead, Rook Security
Jeff Williams, co-founder and chief technology officer, Contrast Security

GONE BUT NOT FORGOTTEN

WHATEVER HAPPENED TO APPLE V. FBI?

SC Media throws it back to February 2016 when Apple and the FBI squared off for a contest that never happened. The immediate issue was temporarily resolved, but the controversy never died, Teri Robinson reports.

This time last year the FBI and Apple were spoiling for a fight in what promised to be an epic battle between privacy and government overreach. No sooner had the two suited up and laced their gloves, than the battle fizzled out after the FBI used a third party to crack the iPhone 5C used by San Bernardino shooter Syed Rizwan Farook that was at the heart of the controversy.

Soon after, another high-profile case involving access to an iPhone – as part of a drug investigation in Brooklyn – came to a screeching halt when authorities got the password for that phone from an outside party.

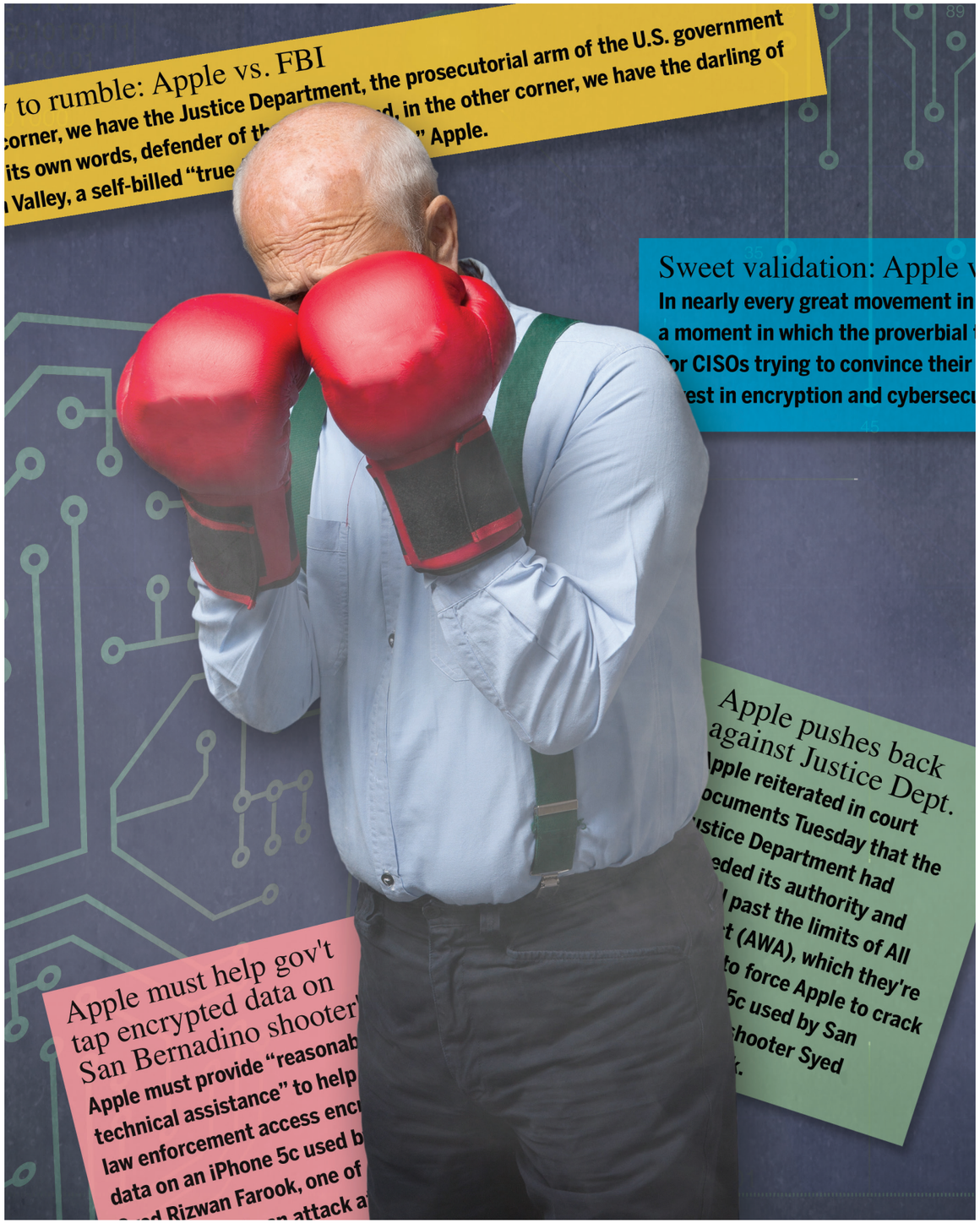
Despite those positive turns of event, Apple – and other tech companies – couldn't take off on their victory lap. Though it was eclipsed by the tumult of the presidential election – Hillary Clinton's use of a private email server, the swell of allegations that Russia interfered in a sacrosanct democratic process, and a furiously tweeting president-elect sucked up much of the air in the room – the debate at the center of the Apple-FBI dust-up is still brewing.

"The FBI found a way to crack iPhone without Apple's help," explains Trevor Hughes, president and CEO of the International Association Privacy Professionals (IAPP). "So we never got a legal judgment."

What the industry did get, though, was a hint at policy to come. "An enormous amount of consensus emerged that a backdoor in an encrypted system is not good, it creates a key" for access, says Hughes. "Any backdoor creates a security risk." The public, activists and some lawmakers rightly assessed that leaving a way in for even the most upright of democracies would open it up to national and intelligence initiatives of more nefarious governments and organizations.

Apple CEO Tim Cook was overwhelmed with the initial response from a wide swath of the public. "Over the past week I've received messages from thousands of people in all 50 states, and the overwhelming majority are writing to voice their strong support," he wrote at the time in a letter explaining why Apple wouldn't cave to the court order mandating it heed the government's request for help in the San Bernardino case. "One email was from a 13-year-old app developer who thanked us for standing up for 'all future generations.' And a 30-year Army veteran told me, 'Like my freedom, I will always consider my privacy as a treasure.'"

Indeed, a Thycotic survey of 250 Black Hat Las Vegas attendees shows similar support for the Cupertino,



Calif.-based company's position. Nearly half, or 45 percent, think the U.S. government has been hacking and spying on citizens' personal data for a very long time, but only now has come to light. And four out of five respondents believed Apple was in the right.

Cook, personally, has drawn praise for standing strong. "Tim is unwavering in his support of an individual's right to privacy," Rep. John Lewis (D-Ga.) wrote of Cook last year in Time's 100 Influential People. That's high praise indeed, from the noted civil rights leader who as a young man marched with Martin Luther King Jr. over the famed Pettis Bridge in Selma, Ala.

Tech companies and their leaders that don't show similar backbone might find potential customers hesitant to purchase their products, a panel at SC Congress in Atlanta agreed last spring.

"If I know a company has willingly built back doors into their products, from a purchasing perspective, it's a factor I take into consideration," said Kevin Morrison, head of information security for Jones Day, even if those backdoors are there for maintenance purposes.

That kind of thinking likely shored the Cupertino, Calif.-based company's resolve in taking on the government. Self-described "Apple geek" Gary Phillips, CISO of the Enterprise Infrastructure Services (EIS) division of Time Warner, speaking on the same panel, said he wouldn't "attribute to Apple any high-minded ideas. I think they protected their market."

> "Consensus emerged that a backdoor...is not good."
>
> – Trevor Hughes, IAPP

The Apple case also sparked an uptick in the interest and use of encryption by both vendors and users.

"Encryption is becoming more and more common," says Hughes, though it creates a bit of escalation – intelligence [agencies] want access and consumers want more and more protection."

The last 12 months have given rise to numerous events that will likely test the mettle of Apple and its peers, as well as users, on issues of backdoors and encryption. Expanded NSA and FBI surveillance powers and a new U.S. president who has thus far proved inscrutable on issues of policy but has expressed strong feelings about – and even urged a boycott of – Apple over its resistance to the government's entreaties, threaten to change the landscape.

Privacy watchdogs went on high alert earlier this year, after the NSA was given expanded powers to exchange information gathered in its global surveillance operations. The intelligence organization will now be allowed to share raw data with the federal government's 16 other intelligence agencies.

The Obama administration's order stipulates that communications intercepted by the NSA can be shared before privacy protections are applied. Previously, the NSA was restricted in what it could do with the data collected as part of its surveillance activities.

The alteration means that more government personnel will have access to the intercepted raw data – which includes communications from satellite transmissions, phone calls and emails both in the U.S. and abroad.

When asked whether he believed this new rule to share "raw signals intelligence information" will threaten privacy rights, Nate Cardozo, senior staff attorney at the Electronic Frontier Foundation (EFF), a digital rights group based in San Francisco, told SC Media that indeed, it would.

"This change represents a significant and substantive expansion of the number of people and agencies permitted to access raw, unfiltered, warrantless surveillance data," he says.

The bulk collection of communications data of Americans is taking place today, purportedly under the authority of Executive Order 12333, Cardozo explains.

"That collection violates the Fourth Amendment. These rules don't make the underlying collection any more (or less) unconstitutional."

These rules, especially Section VIII, invite law enforcement to engage in illegal "parallel construction," Cardozo told SC Media. "Warrantlessly collected data is (in essence) laundered and hidden, not just from criminal defendants, but even from courts.

The FBI, too, was granted sweeping new authority to broaden its spying as Rule 41, a new edict proposed by the Supreme Court, was adopted in earnest, granting U.S. judges the right to sign off on warrants outside their jurisdiction.

Whereas judges previously could only provide orders within their own locale (usually spread over a few districts), the new rule would apply to a wider dragnet, even across countries. The intention is to more effectively prosecute cybercrimes which, of course, could originate and spread beyond one particular jurisdiction. But privacy advocates argued that Rule 41 would allow the FBI to expand its surveillance capabilities. An agent would need only to get a judge's signature on a search warrant to put into play the agency's network investigative techniques (NITs), which allow the agency to hack into and monitor any computer or device on the globe.

> "These rules don't make the underlying collection any more (or less) unconstitutional."
>
> – Nate Cardozo, EFF

Top-down surveillance?

As with most issues, where Donald Trump will land on surveillance, government requests and encryption now that he's in the White House is anyone's guess. "Trump has spoken strongly about surveillance," says Hughes, "but he loves his personal privacy."

In February 2016, Trump told Fox and Friends the then-Republican candidate said "I agree 100% with the courts. In that case, we should open it up. I think security over all -- we have to open it up, and we have to use our heads. We have to use common sense."

Days later he called for a boycott of Apple until the company aided the FBI and accused Cook of "looking to do a big number, probably to show how liberal he is."

The EFF points out that Trump was quoted as saying during the campaign that he tended "to err on the side of security" and also spoke in favor of restoring portions of the Patriot Act.

"When you have people that are beheading [you] if you're a Christian and, frankly, for lots of other reasons, when you have the world looking at us and would like to destroy us as quickly as possible, I err on the side of security," Trump was quoted as saying.

He has also called whistleblower Edward Snowden a "terrible threat" and a "terrible traitor.

Hints at how the wind may blow for tech companies and the government going forward may be found in Trump's cabinet, intel and advisory picks.

Sen. Jeff Sessions (R-Ala.), nominated for Attorney General, called out the USA FREEDOM Act, which replaced the Section 215 under the Patriot Act, for making "it vastly more difficult for the NSA to stop a terrorist than it is to stop a tax cheat."

Trump's pick for CIA director, Rep. Mike Pompeo (R-Kan.), in an opinion piece in the Wall Street Journal, called for "a fundamental upgrade to America's surveillance capabilities" and said "legal and bureaucratic impediments to surveillance should be removed."

In fact, surveillance should be taken a step or two or three farther, Pompeo opined, saying, "Congress should pass a law re-establishing collection of all metadata, and combining it with publicly available financial and lifestyle information into a comprehensive, searchable database."

He's had even harsher words for Snowden than Trump, saying the whistleblower "should be brought back from Russia and given due process, and I think the proper outcome would be that he would be given a death sentence."

In January, Russia extended Snowden's asylum by three years, just a day after President Obama pardoned whistleblower Chelsea Manning. Amid findings by the intelligence community that Russian operatives meddled in the U.S. presidential election, Trump has continued to praise the country's president, Vladmir Putin. Whether two will agree or clash on Snowden's fate remains to be seen.

Just how hard – or even if – Trump will press tech companies into action on behalf of his administration's security goals, is also up in air.

Tech pros recently pushed back against Trump's pledge to build a Muslim registry that he says will help curb terrorism. Last December, nearly 3,000 Silicon Valley engineers pledged to not participate in the building of any such registry. "We refuse to participate in the creation of databases of identifying information for the United States government to target individuals based on race, religion, or national origin," they stated in a letter.

They're likely to maintain their stand against providing backdoors into their products as well. But the issue continues to percolate and will do so until the industry gets a legal ruling – whether that will come this year or later depends on whether the Justice Department makes it a priority going forward. ■

BUT, how'd they do it?

After months of spurning the government's advances, Apple found itself in the unenviable position of trying to get the FBI to tell it just how a third-party vendor, said to be Israeli security firm Cellebrite, was able to crack the iPhone 5c that belonged to San Bernardino shooter Syed Rizwan Farook. Now 100 pages of documents released by the bureau in response to a Freedom of Information Act (FOIA) lawsuit purport to do just that...only the documents are heavily redacted and don't reveal much at all.

The Associated Press, Gannett and Vice Media had filed a federal lawsuit asking for details on who the FBI hired to get into the phone, how it was done and how much the agency paid, even while insisting that only Apple could aid lawmakers in providing access.

According to the Associated Press, the documents, marked "secret," revealed that FBI signed a non-disclosure with the vendor and also entertained interest from three different companies.

That a third party was able to get into the phones encrypted files lent credence to the belief that the FBI was hoping to make an example of Apple, using the dispute as a test case to set legal precedent.

A breach at Cellebrite and the theft of as much as 900GB of information also likely proved Apple right in taking a stand against providing a backdoor into its products. In a statement on its website Cellebrite said, "The impacted server included a legacy database backup of my.Cellebrite, the company's end-user license management system."

Product Section

eSentire P35
A very powerful threat intelligence aggregator.

Catbird P42
One of our favorite products and well worth considering.

Intel P48
Actor-centric cyberthreat intel collection

A batch of innovative new tools to get 2017 started

This month, we begin with a look at lopen source threat intelligence tools. That does not mean that we are looking at open source products, though. Threat intelligence can be open or closed source. Open source refers to intelligence that is available publicly. Closed source usually means intelligence in which there is some level of special access needed to get to. So, putting it simply, open source is about coverage and closed source is about access. Open source is the bulk of what we look at but there is a bit of closed source included.

Next this month we take up cloud-based security management. This is a rather small group and the area it covers is growing rapidly. The problem is that once you opt to put your digital assets in the cloud you are faced with several management challenges. If you are in a public cloud, there may be contractual issues that make security management something that requires special care. If you are spread across several public clouds and some are based in foreign countries, you may have privacy challenges that increase the difficulty of managing security in your cloud-based enterprise. If you have a hybrid cloud – some public, some private and, perhaps, some hardware – the challenges multiply.

Each of our cloud-based products this month approaches the market space somewhat differently in that, while they perform essentially the same types of tasks, their focuses are slightly different. For example, some address private clouds, some address public clouds and some address both. One interesting difference between the products we've seen in the past and this month's offerings is that some of those we have been used to seeing have been subsumed by other products or companies.

In addition to our group reviews we revisit two of our SC Lab Approved products after having used them for a year. This is a new feature for 2017. When we designate a product as SC Lab Approved we make it a requirement that we are licensed to use it in our lab for a year. At the end of that year, we do a detailed review of how the product performed over the year. This month we will look at two tools in our cyber and threat hunting stack.

—Peter Stephenson, technology editor

How we test and score the products

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

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

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

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

What the stars mean

Our star ratings, which may include fractions, indicate how well the product has performed against our test criteria.
★★★★★ Outstanding. An "A" on the product's report card.
★★★★ Carries out all basic functions very well. A "B" on the product's report card.
★★★ Carries out all basic functions to a satisfactory level. A "C" on the product's report card.
★★ Fails to complete certain basic functions. A "D" on the product's report card.
★ Seriously deficient. An "F" on the product's report card.

What the recognition means

Best Buy goes to products the SC Lab rates as outstanding.
Recommended means the product has shone in a specific area.
Lab Approved is awarded to extraordinary standouts that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

Emerging products: Open source threat intelligence

It's a good idea to look closely for aggregation since it can add measurably to the depth and breadth of your analysis, says Technology Editor Peter Stephenson.

SC MEDIA EMERGING PRODUCTS

On occassion, Technology Editor Peter Stephenson and his team at the SC Lab address emerging technologies and markets. The purpose is to look at segments in the information assurance space that represent new technologies, needs and capabilities. In those emerging areas there always are new entries and old pros that want to expand into the space. We will be looking at both – and bringing you the companies and products that we believe will shape the future.

This batch is an emerging products focus. We do these a couple of times a year with the idea that we want to keep you current on the newest trends in security tools. This time we look at open source threat intelligence tools. That does not necessarily mean that the tools are open source – although there might be some of those out there (check GitHub for possibilities). Some tools for analyzing open source intelligence also can analyze closed source intelligence. As well, some are intended to process raw data. A free example is Anomali STAXX. STAX is a TAXII client that processes STIX files from TAXII servers.

Many cyber threat intelligence tools are cloud-based. Some require on-premises server support. However, we've found that both types can be quite competent and can give a great deal of good information. Finally, most such tools will take (and, perhaps, give) feeds from/to other sources. So it is a good idea to look closely for this type of aggregation since it can add measurably to the depth and breadth of your analysis.

How does one apply these tools? First, open source intelligence is about coverage and closed source is about access. So for open source tools we need to be sure that we have the best techniques for collecting and processing big data. When we are looking at millions of data sources across the internet, we need a way to manage that flood of data. The flood is coming in all the time so the amount of data grows hugely.

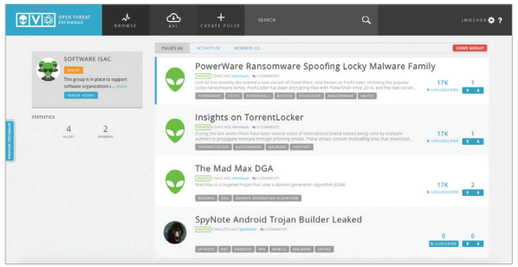
Threat intelligence is used cyclically. What that means is that if we think of threat intelligence tools as being depicted in a circle with the various tools around the perimeter we can enter the circle at whatever point is correct for the snippet of intelligence we want to follow up. There is no such thing as the "big secret". Intelligence is comprised of lots of little secrets that we, as analysts, tie together to get to the answer we seek.

So we start with a seed. That could be a small piece of intelligence - an indicator of compromise, for example - or a question the we want to answer. In many cases of intelligence research in our labs here at SC we start with little more than an IP address. Then, through iterative analysis, we broaden that IP address to a fuller picture. Virtually all of that work can be done with open sources with the expectation that the results could be applied to a closed source search.

For example, we have taken a set of four or five IP addresses/domains plus a couple of email addresses for domain registrants. This rather paltry starting point yielded, through iteration and use of multiple tools, thousands of results that then needed to be culled and de-duplicated to get back to a reasonable stack of needles from which we wanted to extract a single needle.

The tools in this month's reviews are similar to and yet different from each other. So it is completely reasonable that you would need more than one of them to be effective. Look carefully at what you can get from each and craft your kit to meet your objectives. Today much of what you'll do with intelligence tools is manual.

So your tools will make a big difference in your productivity and response time. Remember, the purpose of intelligence is making your defense mechanisms more and more proactive. Tools that process STIXX files will, in the not very distant future, feed defensive tools directly, taking you out of the loop and allowing a much faster response to the rapid changes in the cyber threatscape.



AlienVault

Open Threat Exchange (OTX)

DETAILS

Product Open Threat Exchange (OTX)

Company AlienVault

Web alienvault.com/otx

Price No cost.

What it does Collects indicators of compromise from a very large user community and makes them available in a wide variety of ways.

What we liked Completeness of the data and flexibility of the ways to use it.

The AlienVault Open Threat Exchange (OTX) is among our most useful threat intelligence tools. It is an open source of indicators of compromise (IoCs) supported by the community. That community comprises both AlienVault users and those who are not customers of AlienVault. If you own an AlienVault appliance, however, you can both consume and automatically contribute what the company calls "pulses." At this writing there are 24,000-plus users who have contributed over 792,000 indicators in more than 6,000 pulses. Each pulse contains a collection of IoCs targeted at a particular focus. For example, during the recent frenzy over Grizzly Steppe there were six pulses contributed over the course of four days.

Access to the OTX is through URL https://otx.alienvault.com/browse/pulses/. Once in the tool you can browse pulses or search based on adversary, author, pulse, industry and several other parameters. You also can subscribe to particular users and groups so that you receive emails of new pulses contributed by those entities. If you wish to contribute pulses, you can create an account at no cost.

Indicators can be of just about any type that we commonly associate with IoCs. The OTX recognizes, among other types, the usual IPv4, IPv6, CIDR address blocks, CVEs, domains, hashes, email addresses, hostnames and URI/URLs.

Another benefit of the OTX is the ability to construct a campaign out of indicators of compromise. In STIX-talk, a campaign has indicators, observables, actors, etc. All of these elements may be available on the OTX depending on the contributions of the community. However, using a STIX editor, such as Soltra Edge, these components can be stitched together to form a rudimentary campaign. The draft campaign can then be enriched by future pulses and data from other sources. The result is a complete picture that can be used to pre-load defensive devices with data needed to fend off attacks based on the campaign in the future.

But the usefulness of OTX in that regard does not require the complete data for a full campaign. Any indicators may be quite useful when protecting your enterprise. Whether used with AlienVault products or exported in a format that other tools can consume, the indicators in the pulses on the OTX are valuable and in a form that is easily consumable.

We like the tool and it is one of the staples in the SC Lab. For more detailed information about the AlienVault Open Threat Exchange (OTX), go to the site for the user guide.

eSentire

CYMON.io

This is another of our workhorse tools. Cymon is an open source threat intelligence aggregator. It ingests over 180 sources daily to track malware, phishing, botnets, spam and more. Over 20,000 unique IPs are added to the Cymon database every day. To date, Cymon has logged more than six million IP addresses and more than 33.7 million security events. In the SC Labs we use Cymon to backstop virtually all of our other tools.

When we identify an IoC in one of our tools, we generally test the indicator in other tools to ensure that we have all of the data about it. Cymon is, invariably, our first stop. However, there are many times that we are made aware of an indicator and it does not appear in one or more of our tools. In that case, it is a fairly certain bet that Cymon can tell us something about it.

At its heart the tool is a very large database of threat intelligence data. Those data can be searched by IP, domain, URL or hash. When performing a search, a lot of information may be available. We say "may be" because Cymon extracts its data from a wide variety of sources. The information those sources provide dictates the information that Cymon can provide to you – with one exception.

That exception is the set of intelligence lists from eSentire, the organization that supplies Cymon. Those data add significant enrichment to the data from outside sources. The end result can be anything from tantalizing tidbits on a very new indicator to a complete history, perhaps with malware details, for more mature indicators. So, given that Cymon has access to its own dataset, it really is far more than just an aggregator.

This dataset – both the eSentire source and the external sources – allows a rather thorough historical analysis of an indicator. It really does not matter what your reason for analyzing an indicator is - phishing, malware, breach, etc. – the data very likely will be there. For example, we took an IP indicator from the Grizzly Steppe collection and put it in Cymon.

The tool returned with data from several reporting sources: botscout.com, labs.snort.org, tor.dnsbl.sectoor.de, xbl.spamhaus.org, dnsbl.httpbl.org, zen.spamhaus.org, cbl.abuseat.org, and urlquery.net. These are the reporting sources for the indicator we searched. It showed a timeline going back to May of 2016 and there are links to the specific findings of each of the data sources.

This is an excellent tool – certainly, the price is right – and it has, as you can see, a lot of capabilities. Add to that a full set of REST APIs and you have a very powerful threat intelligence aggregator.

DETAILS

Product CYMON.io

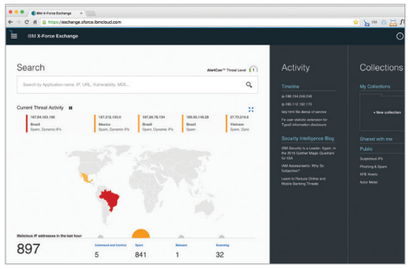
Company eSentire

Web cymon.io

Price No cost.

What it does Threat intelligence aggregator.

What we liked Uses so many sources that it is very likely to have information that other single sources don't have. Very easy to use.



IBM Security

IBM X-Force Exchange

The IBM X-Force Exchange (XFE) grew out of the old Internet Security Systems, one of the pioneers in information security lore. Today, the X-Force Exchange is a repository for IBM Security intelligence, both collected and in near real-time. It has the interesting feature of allowing users to create their own collections of indicators as well as accessing other collections. It does this by timelines, blogs and public collections.

The tool can be searched by application, IP, URL, vulnerability or hash value. It tracks trending indicators and monitors current threat activity which it displays as a rolling ribbon on its landing page. The timeline covers indicators and includes the ability for users to comment. Clicking on an indicator in the timeline takes users to the X-Force report and comments.

Overall, we didn't see a lot here that isn't available on a host of other products. Nonetheless, it's an interesting resource and we have known it to have information that no other resource has. To that end, we deem it a valuable tool.

Exchange has two dashboards: the classic dashboard and the "new" dashboard. We prefer the new dashboard because it is far easier to navigate and has a lot more information than the classic. Expanding a collection gives access to the elements of the collection which can be referred to or downloaded in STIX format.

Unlike most other cyberthreat intelligence tools, XFE includes vulnerabilities. For example, a cross-site-scripting vulnerability in the AContent CMS was added on December 31. The details are a bit thin but the vulnerability is covered and it references CVSS 3.0.

XFE also is a distribution point for X-Force advisories. We picked an advisory on the GozNym malware and found the description complete and useful. However, we would have liked to have had more information about the included malwares as represented by its hashes.

But, when we selected a collection of botnet command-and-control servers, the results were markedly better. In this one there was a pair of linked collections, one for the Mirai network and another command-and-control botnet collection.

Overall, while XFE is a good concept and there is a long history of significant expertise at play, we believe that it has a way to go. We are not sure why it has not taken off, given that IBM sponsors it, but it may be that its overall user-friendliness is a bit lacking. That said, we certainly did not find it onerous and it may also be that this is one of those tools maintained largely by its owner and used for reference by the community rather than experiencing a lot of community contribution.

DETAILS

Product IBM X-Force Exchange

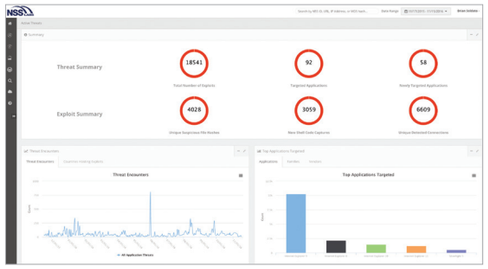
Company IBM Security

Web exchange.xforce.ibmcloud.com

Price $0.00 for on-platform queries, $0.00 for API access up to 5,000 records per month. For API usage over 5,000 record monthly limit, pricing is $2,000 per 10,000 records per month for a commercial API subscription.

What it does Cloud-based threat intelligence resource.

What we liked The strong resources of the IBM X-Force behind the intelligence collections and the near real-time monitoring of a huge body of data points around the world.



NSS Labs

Cyber Advanced Warning System

CAWS is an interesting product. It is designed specifically to answer some powerful questions: (1) Am I at risk of being breached? (2) How can I compare my defensive measures to decide if I have the competitive intelligence that I need? and, (3) How do I gain complete visibility of exploits across all assets within my environment from a single interface?

CAWS is a unique application that mimics a human operator so you have an active honeypot rather than a passive honeypot. It also can mimic vendor product stacks and compare efficiencies. The vendor refers to the CAWS source capture/crawling and the "bait net." The tool focuses on exploits, mostly malware, and follows the kill chain. However, since everything CAWS sees is recorded you can go back and analyze an attack from start to finish.

CAWS uses data gathered by NSS Labs rather than monitoring your enterprise directly. However, it collects a huge amount of data. You enter a sort of profile of your network. This profile contains the applications, profiles and security products that you select from over 350 options. These represent what you have in your enterprise. As you monitor this profile you learn immediately what NSS Labs has learned about attacks against each item in your profile, the threats that have bypassed your defenses and what you should do about them.

In addition to your profile, CAWS monitors a large number of known malicious URLs. But you can add your own URLs for analysis. We dropped into the dashboard as our starting point. This gave us a summary of applications exploited, total active exploits, URLs hosting exploits, exploits bypassing security products, exploits blocked by security products, total application families targeted and top platforms targeted.

CAWS is available at no cost for single users. The enterprise version is reasonably priced and gives several additional capabilities above the free version. This is not a tool to be considered a replacement for defensive devices. Rather, it is a pure-play intelligence tool.

We liked this tool largely because it lets us track many of the risks associated with threats and vulnerabilities in our enterprise. That is not to say that we should stop vulnerability assessments or pen tests. It simply gives us a tool to be proactive. For example, knowing in advance that our firewall has some discovered weaknesses to specific attacks is useful. Because CAWS lets us see the compromise path for a discovered weakness we can look at the path within our enterprise and take all reasonable measures along the whole path – including on the device itself.

DETAILS

Product Cyber Advanced Warning System (CAWS)

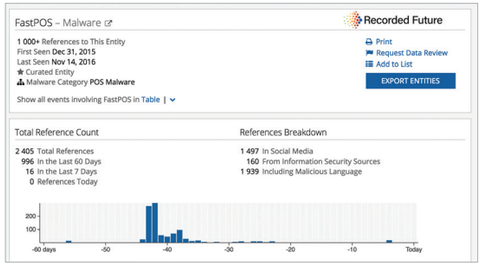
Company NSS Labs

Web nsslabs.com/caws

Price CAWS is free. CAWS Enterprise is $5,000 annually or $500 month per seat (user).

What it does Threat intelligence centered on device and application susceptibility to threats as well as malicious URLs.

What we liked Ease of use, comprehensive view of the devices and applications in our environment.



Recorded Future

Recorded Future

One of the things we really enjoy about emerging products and First Looks is that from time to time we encounter something really cool that we've never used before. Under our tree this year we found a most interesting and, it turns out, most useful threat intelligence product, Recorded Future. We have been receiving the free Recorded Future Cyber Daily Plus reports for some time and they frame our day's reading each morning. But for this set of reviews we got to exercise the full product and we were impressed.

The thing that is most impressive about Recorded Future is the breadth and depth of their coverage. The landing page at first blush is way too busy but at second blush it magically organizes itself and makes perfect sense. What starts out looking like a big, disorganized table really is a set of five very well-organized columns that let you drill down into attackers, methods, targets, operations and indicators. You can scroll down each of these columns, pick something of interest and drill further to get a lot of underlying information.

No wonder that there is so much information available. Recorded Future claims to have the world's largest SaaS platform targeting over 750,000 sources, including forums, paste sites, blogs and social media, over 30 threat feeds, a TOR collection with hundreds of new pages added daily, code repositories and technical collections. It is a prodigious resource. All of this comes from over seven years of collecting. That also gives a solid historical picture as well.

That's the good news. The not quite so good news is that to really make this tool sing you need to spend some time with it. To make that painless, Recorded Future sends daily emails after you sign on for the first time telling you what to do next. In less than a week you're an expert.

Since Grizzly Steppe is the hot button at the moment we dug into it by clicking on it at the top of the Operation column. To our surprise, we not only got all of the tool's intelligence on the operation, we were told that there are over 5,300 references to it and there are seven that predict activity over the next 30 days. Mousing over the operation we saw that every item in every column that relates to it was highlighted. Clicking on the operation took us to a drop-down and from that we were able to see everything that relates to it on a single screen.

Overall, we see this tool as a "must have" for any serious threat analyst. Pricing is variable depending on configuration. In addition to the basic system, Recorded Future can integrate with a variety of third-party devices, such as SIEMs, and services such as Maltego. It has a dedicated service for addressing the Dark Web.

DETAILS

Product Recorded Future

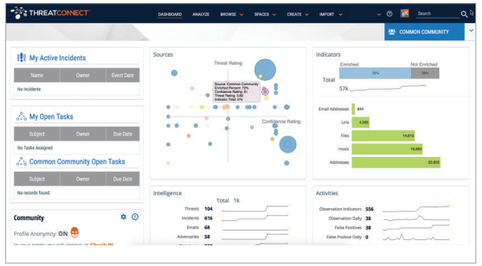
Company Recorded Future

Web recordedfuture.com

Price Depends on configuration, etc.

What it does Cyberthreat analysis on steroids.

What we liked Comprehensive and detailed, current as well as historical data, just about everything a cyber intel analyst needs in one package.



ThreatConnect

(free version)

If you depend on first blushes and getting-started guides, you won't give this one a second glance. And you'd miss a big opportunity to dig into a very nice open source intelligence tool that has a great price: free. This is a good community-supported threat intelligence tool with a lot of power – albeit most of it, sadly, too well hidden. So, take your time with this one and roam around, click things, test it with real use cases. You'll be glad that you did. We used the Grizzly Steppe data for testing as we did with all of the other tools we looked at. The results turned out – after a half-hour session with the vendor – to be well worth the effort.

When you hit the landing page/dashboard, you'll find the usual mix of statistics, commentary by the community of users and a bunch of links. The commentary is interesting but its real value is that the community contributes indicators to the Common Community pool. If you've been working incidents, the history of your searches will appear on the dashboard, as will a list of your active incidents.

Layout is very clean with a number of menu choices across the top of the screen. We started with the Analyze menu. This brought us to an input page so we uploaded a text file with our Grizzly indicators. You can type in individual indicators or upload text, PDF, DOC, DOCX, PPT, XLS and XLSX files directly. You can even edit the list in place, if necessary. Clicking Next brought us a list of all of the indicators in our list that ThreatConnect knew about already. We picked the first entry in the list for further investigation.

There were three skulls next to it meaning that it had a score of 3/5 for threat level, and a 100 percent next to the skulls meaning that the threat rating was a 100 percent probability of being correct. On the far right of the entry was a number, 300, meaning its risk score was 300/500. We next expanded the Common Community for this indicator and selected Attributes. That gave us sources and descriptions of the indicator. Clicking on the Incidents choice got us a record that we could click and expand. This took us to an entirely new level with menu options of Overview, Tasks, Activity, Associations, Sharing and Spaces. The Overview page has lots of good information.

Finally, ThreatConnect supports STIX/TAXII. This is a major benefit and one we hope to see more and more frequently. This is a very good, free tool for analyzing open source intelligence. Don't be put off by the bare bones documentation. The more you root around in the tool the more you'll find. The Help function takes you to a lot of info for training and documentation. Just have patience and enjoy the ride.

DETAILS

Product ThreatConnect

Company ThreatConnect

Web threatconnect.com

Price No cost.

What it does Cloud-based cyberthreat analysis tool.

What we liked Very good drill-down and lots of flexibility. Huge number of free threat feeds and a good community of contributors.

Cloud-based security management

As you select a security management system for your cloud/virtual space, the answers are not always straightforward, says Technology Editor Peter Stephenson.

PICK OF THE LITTER

GuardiCore Centra is a solid tool for managing the security of a software-defined data center. It is easy to set up and use and visualization is excellent for rapidly analyzing an incident. This is one of the best tools of its type that we've seen. It is comprehensive, reliable and easy to use. We make it our Best Buy this month.

FireMon FortyCloud is a powerful tool with a very clear and important mission that it fulfills well. We make this our Recommended product this month.

SC MEDIA BEST BUY

SC MEDIA RECOMMENDED

SC MEDIA LAB APPROVED

The growth of the software-defined data center demands a software-defined solution for the problem of managing the security of cloud environments that are unique to the organization. While the generalized architecture of a cloud-based enterprise may be fairly well understood, in fact each enterprise is different. This is no real change from the traditional hardware data center. One size never has and, likely, never will fit all. That demands a level of flexibility in management – and, especially, security management – schemes. That's the bad news.

The good news is that the software-defined data center offers a lot of flexibility and a good cloud-based security management system can have equal flexibility. That is what this month's products are all about. Their job is to manage the security of a cloud-based enterprise, no matter how complicated, geographically disbursed or diverse in its privacy and security requirements.

It used to be that we thought of clouds as public, private and hybrid. While that still is true, it's a bit more involved today. For example, part of the enterprise might be in one public cloud, one in another, and there might be a virtual environment in the organization's data center. All of these environments must work together, efficiently and securely.

Carrying the use case a bit further, consider that the part of the software-defined data center that is in the virtual environment on premises contains sensitive data, while the other two – the ones in the public clouds – contain applications and data that is not as sensitive. But – and here's where one of the common challenges appears – the cloud applications must access the sensitive data for some people from partiicular locations due to international privacy laws. How do you manage all of that? Again, that's where this month's tools come into play.

To be effective, the tools must, themselves, be in the cloud. However, there are some combinations of "in the cloud" and on premises that work well, too. Another consideration is where – if at all – you place either sensors or agents. That, of course, depends on what you are trying to control. If you are largely interested in network device configuration, then you might want sensors.

The next consideration is what you want to manage. Think of what you would want to manage in a hardware data center. Some things that you might like to manage in a hardware environment are a bit awkward, but in the cloud, it can be a lot easier. Before you start thinking about which tool set you want, figure out what you need to have it do. Don't forget that, at the rate things are maturing today, change is inevitable, so you want to be sure that you can grow as your software-defined/cloud-based enterprise matures and grows.

Laws are changing rapidly as well. If you are an international or multinational organization, you may need to address privacy laws in the EU. As the EU, by some accounts, begins to unravel, laws that affect how you secure PII will certainly become more complicated. So be sure that you can accommodate changes that are very difficult to anticipate.

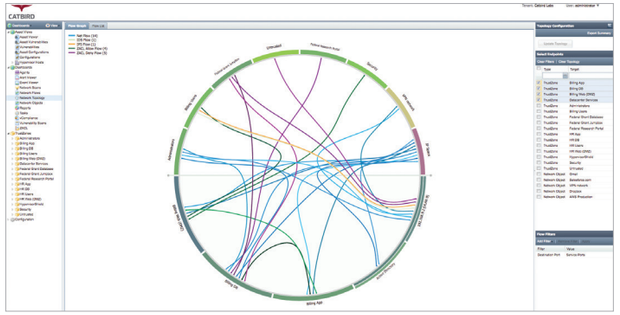
Finally, we are seeing a trend toward supporting fewer and fewer legacy applications, including operating environments. Be sure that you can move forward in that environment without having to rip and replace your management system. Along with that comes the proliferation of operating systems. In the case of the virtual environment, what is your hypervisor and will your choice of a management system accommodate it (does it need to, and if so, how?) as well as a potential switch in the future? Equally, what is your choice of cloud and will your management system keep up with your choice(s)?

All of these are important questions to ask. We noted that some of the tools we looked at were pretty close to being point solutions. So you may need to consider more than one tool set to get your particular job. That is not always optimal since you will have multiple panes of glass, something that most SOC/NOC teams are trying to avoid.

Specifications for cloud-based security management tools

●=yes ○=no

Product	FireMon	GuardiCore	CloudPassage	Catbird
Scalable secured connectivity to the cloud	○	●	●	○
Microsegmentation	●	●	●	●
Adaptive automation	●	●	●	○
Dynamic analytics across entire cloud footprint	○	●	●	○
Deception network	○	●	○	○
Honeypot	○	●	○	○



Catbird
Secure

Catbird Secure enables automated enforcement of security policies, including microsegmentation rule sets, across Catbird TrustZones. The platform detects and alerts on potential security incidents, initiates corrective enforcement actions, provides instant compliance reporting for major standards and allows users to visualize/analyze virtual lateral traffic patterns.

Virtual machine appliances (vMA) are installed on each hypervisor and communicate securely with a control center. The resources for a vMA start at 4GB of memory and 2 vCPUs. Control center requirements start at 8 GB of memory and 4 vCPUs.

We dropped into the landing page, which contained an inventory of virtual machines in the software-defined data center. The VMs are arranged into trust zones. Policies are applied to the trust zone and they affect each of the VMs in the zone. The VMs are monitored on layers 2-4 as correlated with the hypervisor. Hypervisors supported are VMware, OpenStack and soon Amazon AWS.

In addition to Catbird Secure, there is a read-only version called InSight. The purpose of InSight is to monitor the same things that Secure does – but without permitting changes to be made. Once you have your trust zones set up, you can move to the graphical interface. This is an impressive page. The GUI shows a wheel with trust zones around the perimeter. Within the wheel there are color-coded connections between zones showing the flow activity at any given time.

The color-coded lines are generated automatically based on raw flows between endpoints. An example might be flows showing that a firewall was misconfigured. That could mean a failed or blocked connection or a connection that should not have been allowed. You can use the ingress-egress mappings to set up microsegmentation policies. Heavy filtering is available so you can customize with just about as much granularity as you need.

We really liked the visualization on this one because it is clear and instantly readable. Spending a bit of time to get used to it and how your enterprise looks when it is behaving will pay big dividends in being able to spot an anomaly quickly and effectively. We also liked the ease with which trust zones could be characterized with friendly names. It seems that just about everything about this tool is designed to make it faster and easier to spot anomalistic behavior on your enterprise.

One of the important uses of trust zones and whitelists is that you can apply policies to the zone rather than having to focus on individual assets.

Catbird Secure can integrate with a SIEM and can be operated "headless" so that the SIEM provides the user interface. However, we like the tool's visualization and we probably would not use it in a headless environment.

DETAILS

Vendor Catbird

Price Annual license: $2,500-$4,000 (average) per hypervisor. Pricing varies based on environment size, platform, and third-party integration options.

Contact catbird.com

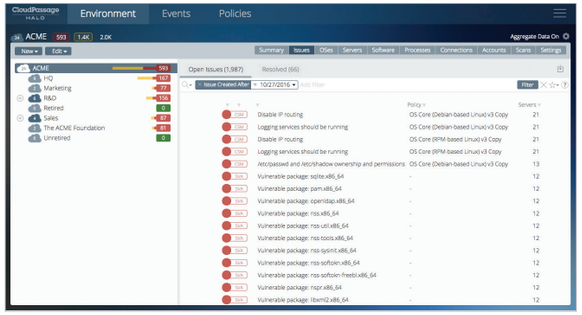
Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★¾

OVERALL RATING ★★★★★

Strengths Excellent visualization and ease of use.

Weaknesses Pricing is a bit convoluted and the support, if one selects the Gold option, could get quite pricey we believe.

Verdict This has long been one of our favorite products and it is well worth considering.



CloudPassage
Halo

CloudPassage Halo is designed to provide cloud workload security and compliance monitoring for public, private, hybrid and multi-cloud environments at enterprise scale. It focuses on the foundational cloud workload protection strategies, outlined by Gartner as configuration and vulnerability management, microsegmentation, traffic visibility and workload integrity monitoring.

Halo automatically applies security policies predicated on the workload type, regulation category or sensitivity of the data. It also scans for software vulnerabilities referencing a number of sources, such as the NIST CVE database. Configuration of workloads use standard benchmarks from the Center for Internet Security (CIS) and the Defense Information Systems Agency (DISA).

The tool performs three fundamental tasks: reduction of the software attack surface, reduction of the network attack surface and monitoring for compromise. You begin by deploying micro agents on every server that you wish to protect. The agents talk to the Halo security orchestration engine which, in turn, communicates with the portal and, through a REST API, with various SOC systems, such as Splunk or GRC systems. The tool supports private clouds and data centers, and infrastructure orchestration from third-party vendors such as CHEF and Puppet. It can reside in public clouds as well, supporting such public clouds as Amazon, Google and Microsoft.

This is absolutely an asset-centric tool in that it focuses on servers. The first task when you go to the landing page in the portal is to set up your environment. You do that by going out from your selected server(s) to the Halo portal and downloading the appropriate script to set up your servers with their micro agents. We selected a Windows Server 2008 and the setup was simple and straightforward. After we registered we simply logged into the portal from the server we wanted to configure. The rest was almost automatic.

Policies are available and are easy to edit. This is a typical policy modification exercise. Save a desired policy, edit the saved copy and deploy it. There are a lot of out-of-the-box policies, though, that you can use as-is. Next, you'll want to scan your assets for compliance with your new policies. Finally, you can perform appropriate remediation. All of this step-by-step is available on the website in the Halo quick start and tour.

We found the pricing on Halo to be attractive. Basic support is included and there are premium support levels available. The website has a good support portal with an FAQ and document library that includes manuals.

Overall, we liked this product. We liked the lightweight agent as it did not appear to interfere with our test server, hardly making a dent in its performance. As long as you automate the deployment, you'll be fine with this one.

DETAILS

Vendor CloudPassage

Price Starts at $350 per package per year.

Contact cloudpassage.com

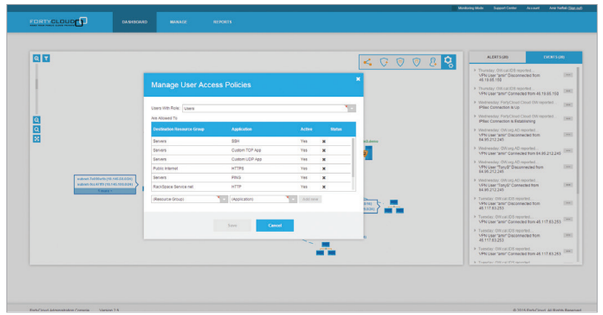
Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★¾

OVERALL RATING ★★★★★

Strengths Solid tool for monitoring cloud deployments, public or private. Very good performance and an attractive price point, although we can see it getting pricey for large enterprises.

Weaknesses Deployment could become tedious. Be sure to plan carefully and use some sort of push tool to deploy agent scripts.

Verdict Good, well though-out tool and, if you are looking for out-of-the-box compliance capabilities, this one demands your attention.



FireMon
FortyCloud

FireMon, the virtual firewall folks, acquired FortyCloud in October 2016 and the addition of an infrastructure management tool that goes beyond the firewall has obvious benefits. This new arrangement between FireMon and FortyCloud certainly is poised to provide those benefits.

SC MEDIA RECOMMENDED

FortyCloud is a cloud infrastructure security broker (CISB) application. This is a type of network security application focused on scaling security operations in public and hybrid IaaS deployments. It provides three general functions: network segmentation and security, abstraction, and automation and orchestration. Each of the functions works with the others to provide comprehensive security management for cloud environments that provide infrastructure as a service.

FortyCloud provides agents and gateways that install in the virtual environment. Gateways provide router and firewall functionality in the form of gateways. The abstraction layer unifies multiple cloud platforms under a single set of policies. That allows administrators to configure policies that will reflect universally instead of needing to recreate policies every time a new device is added to the enterprise. Automation allows automatic discovery of resources and auto-detect changes.

The gateways are installed on Ubuntu servers and any cloud platform is supported. The gateways support most physical or virtual firewalls. FortyCloud uses microsegmentation to perform workload segmentation down to the individual workload level. Once we had the gateway configured – a trivial task, actually – we dropped into the dashboard. Gateways talk to each other and each gateway talks to its own devices, each device having an agent that registers with its gateway.

The landing page, or dashboard, is a network map showing each gateway and the devices it manages. Drill-downs let you manage assets and applications at increasing levels of granularity. Configuration is real-time so if you change a gateway's configuration the change will be reflected immediately in all of the devices. Because microsegmentation lets you micromanage devices and applications against common policies, this really is a one-click configuration.

We found the tool convenient and easy to use. Setup was fast and straightforward. The documentation is a bit more complete than we are used to seeing for cloud-based systems, which usually assume that since there are cloud engineers to support you, you need no docs. We don't agree. When you are connecting something into a complicated environment and that something is intended to manage (or broker) security – such as managing firewalls – it is important to have the documentation necessary to understand what is going on.

DETAILS

Vendor FireMon

Price $195/month (single business gateway license).

Contact firemon.com

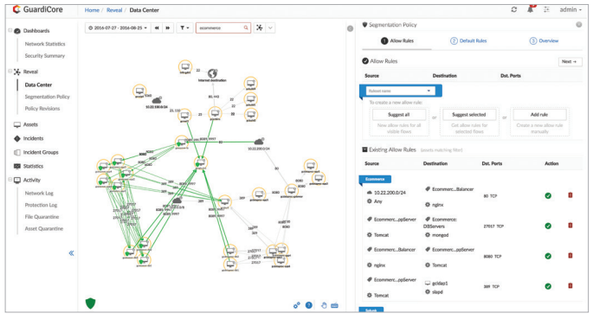
Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★¾

OVERALL RATING ★★★★★

Strengths Easy to set up and changes occur across the managed infrastructure in real time.

Weaknesses A bit pricey for premium support.

Verdict A powerful tool with a clear and important mission that it fulfills well. We make this our Recommended product this month.



GuardiCore
Centra

GuardiCore approaches software-defined data center security from the perspective of five capabilities: flow visualization, microsegmentation, breach detection, automated analysis and incident response. Centra uses a three-tier architecture to address these five capability areas. The tool uses collectors on the hypervisor combined with agents for virtualized assets. It does not matter where the asset resides.

SC MEDIA BEST BUY

Data from agents and collectors are aggregated in aggregation servers. Management servers manage the entire process and house a deception network. GuardiCore is well-known for its deception network and with Centra the company has added additional capabilities without losing the benefits of an advanced deception network. Centra supports most software-defined enterprise infrastructures, including public clouds, bare metal and containers such as Docker.

All of the collectors converge in a single management center. The first thing we noticed was that, although we were seeing traffic between the internet and the enterprise, we also saw internal – or, east-west – traffic. By setting baselines of expected traffic we can alert on unwanted traffic that might represent an intruder in the network. This is the network statistics dashboard and it is pretty much what you'd expect. Drill-down is good and there is a lot of information here.

The other dashboard is the security summary. This gets down to a fair bit of detail, showing which assets are at risk, external attackers, honeypot incidents (from the deception network), external attackers and top services and operating systems.

Moving from the dashboards to the Reveal menu we started with a graphical representation of the data center. This is a flow map and it is extremely useful and lets you see all of the traffic patterns in your network, both internal-external and east-west.

The data center flow map has some strong filtering available that helps build microsegmentation policies for automating analysis. Building segmentation policies is an easy point-and-click proposition. You specify source, destination and destination ports and you have a policy.

This is a pricey product, but it is worth every bit due to its capability and, particularly, the way it can speed up analysis and incident response. The solution can integrate with other tools for such things as reputation and sending indicators of compromise in a form that other security tools can consume. The reputation service – a combination of its own and third-party services – works on files, IPs and domain names. The offering lets you create whitelists and form groups using fuzzy matching.

The website is solid and the documentation is clear and well presented.

DETAILS

Vendor GuardiCore

Price Starts at $25,000 per year; pricing based on number of protected assets.

Contact guardicore.com

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

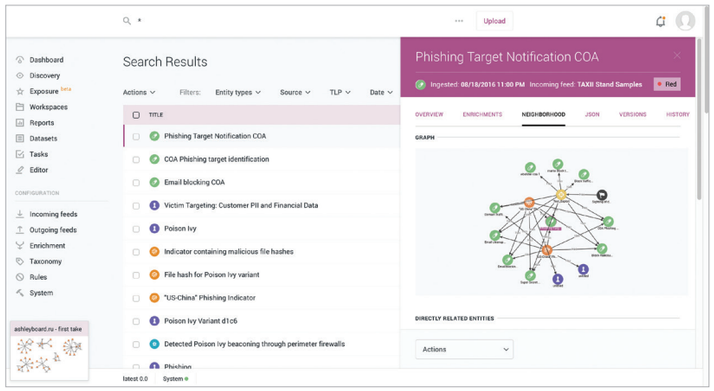
OVERALL RATING ★★★★★

Strengths Solid tool for managing the security of a software-defined data center. Easy to set up and use. Visualization is excellent for rapidly analyzing an incident.

Weaknesses None that we found.

Verdict This is one of the best tools of its type that we've seen. It is comprehensive, reliable and easy to use. We make it our Best Buy.

EclecticIQ
EclecticIQ Platform



We have taken a stand in the past relative to STIX and TAXII. We believe that these are at the top of the list when it comes to cyber intelligence interoperability. Sadly, there are not yet a lot of devices that accept STIX files. There are more today than there were yesterday, though, and there will be more tomorrow. So the trend is in the right direction. What is needed, among other things, to push this along, though, is a growing collection of devices that can both consume and create STIX files. This month's First Look is exactly that. And it is exactly that on steroids.

The EclecticIQ Platform addresses STIX head on. We have been watching the evolution of this tool for a while and for what it is intended there is pretty much nothing around that can beat it. What it does is act as a "combiner" (our unofficial term) for a large number of cyber threat analysis sources. It then applies a lot of smarts to analysis, correlation and normalization of the data. It supports a variety of formats – including STIX 1.0, 1.1.1, & 1.2, XML and JSON, PDF and text.

One of the features that we particularly liked is that the tool is characterized as "analyst-centric." There are a lot of tools of various types that can do a good job of assisting analysis but not quite as many that do everything from the perspective of the threat intelligence analyst rather than the information security professional. As you browse through the screens and reports, one of the first things that you'll notice is that they present information in an easily consumable way. You don't need to be a network or IT security guru. In fact, in some regards, it's better if you aren't.

Either way, this is a solid collaborative tool so – at some level – just about everyone can play and get solid benefit.

We dropped into the dashboard and, as one would expect, we got a broad picture of threat activity from the actor perspective. Then we took a look at the available feeds. We had several incoming feeds and we can add more. Drilling down we can adjust what feeds we have. EclecticIQ provides lots of feeds but if something is missing you can add your own. This is especially useful if you have a proprietary feed that your organization is generating.

Of course we were concerned about what it was able to do in our environment. A little more drilling and we found ourselves in a full-fledged threat hunt. A new feature is the dif capability so we could see how the threat had progressed through our enterprise, if at all. That is just part of the ability the tool has to help you smarten up your analysis. There are a lot of enrichment options and you can create your own rules.

We really like this tool and we've been following it long enough that we feel comfortable designating it SC Lab Approved. We'll slot it into our threat hunting stack and add one more dimension to our analysis capabilities that appear in the Threat Hunter Blog.

– Peter Stephenson, technology editor

AT A GLANCE

Product EclecticIQ Platform

Company EclecticIQ

Web eclecticiq.com/platform

Price Depends on configuration.

What it does Cyberthreat intelligence analysis.

What we liked This is a solid tool with a huge amount of capability in an analyst-centric user environment. We really like the large number of intelligence feeds that it can handle, its solid analysis capabilities and, especially, its use of STIX and TAXII.

The bottom line Even if you already have some threat analysis tools in your security stack, you should take a very close look at the EclecticIQ Platform. It is quite likely to add yet another dimension to your analysis, almost no matter what else you are using with it. Your threat intelligence analysts will love it. We make this SC Lab Approved for 2017.

We take another look at a premier tool
Silobreaker Online

We've been using Silobreaker for over two years. We used it when we supported Superbowl 50 and we've been using it as we research our Threat Hunter blog. It has become the staple workhorse for researching open source intelligence here in the SC Lab. It is our workhorse for two reasons: It is extremely comprehensive (which gives us deep context for any cyber threat research we are conducting), and it lets us set up a dedicated custom search dashboard in minutes.

We have several use cases for Silobreaker. First, we use it for ad hoc research. Because it goes far beyond cyber intelligence we can put the cyber pieces in context with business, government or other environments that may interact with the cyber pieces we are seeking. In short, that lets us see cyber as it fits into a bigger picture and that enables us to answer the important question, "so what?"

Our second use case dips into Silobreaker's alerting. We have set up search dashboards for intelligence threads that we are tracking on an ongoing basis. That lets us wake up every morning to the important events that have happened in the past 24 hours.

Silobreaker has several different formats in which to deliver its results. It has, of course, the expected summaries of items it finds in its searches. But it also has a network display that correlates information in an easy-to-understand graphical interface. There are specific summaries – such as blogs or social media – and, of course, you can drill down to get the full story.

In short, our year with Silobreaker has been rewarding. We have worked closely with the Silobreaker team to provide input as they continually update the product. Because it is cloud-based, we can use it from anywhere that we can access the internet. That lets us use it for training on threat hunting and cyber intelligence analysis.

We recommend this tool and award it the SC Lab Approved designation for the coming year. Support is excellent and the product is in a constant state of updating to accommodate customer needs and to improve the sources it uses for intelligence gathering. Nothing on the internet is static and Silobreaker uses that to its advantage. We never have been confronted with a search that it couldn't do with good-to-excellent results. While it may seem pricey at first blush, it actually is at the low end of prices for similar – not as competent – products. Well worth the money!

– Peter Stephenson, technology editor

DETAILS

Product Silobreaker Online

Company Silobreaker

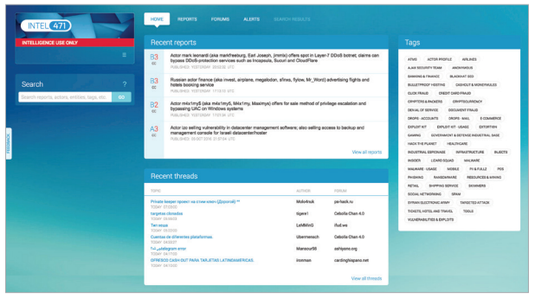
Web silobreaker.com/products

Price From $37,500 per annum.

What it does Open source intelligence.

What we liked Ease of use, completeness of available information, huge database and rapid customization.

The bottom line In our year-plus of in-lab use we have found this to be our open source intel workhorse. No cyberthreat analyst should be without it. The price is cheap for what it can do for you.



We take another look at a premier tool

Intel 471

If our other "One Year Later" product was our open source workhorse [*page 47*], this month's is our closed source go-to tool. We have been using Intel 471 in the SC Lab for well over a year. Before that we used it in teaching intelligence concepts on the university level and in preparation for supporting Super Bowl 50 security. There are a lot of threat intelligence tools – and we use several of them in the SC Lab – but this one is unique in that it focuses on threat actors.

Intel 471 also is unique in the way it was set up as an organization, the way it gathers its intelligence and the core skill sets for many of its team. First, Intel 471 is an intelligence provider. It is not a technically-oriented group. It is a team of intelligence pros from around the world gathering cyber intelligence in the tradition of government intelligence teams. Second, it gathers intelligence in a variety of ways – from being on the ground in closed/vetted forums to direct contact with threat actors and associates of threat actors. Finally, being intelligence professionals, Intel 471 team members know how to separate actionable intelligence from rumor of mis- and/or dis-information.

Intel 471 reports look like traditional intelligence reports in many ways. They usually consist of the report, the researcher's comments, the sources of the information, the indicators that will allow the intelligence to be verified and the Admiralty Code that lets the reader know how reliable the information in the report is and how confident the researcher is of the information presented.

Generally, we couple the closed source intelligence from Intel 471 with open source intelligence from our other tools to get a complete picture, often through Maltego, our internet link analyzer for which there is connection to the Intel 471 API. The result is a full picture of our actor and their activities as seen by all of our tools. By iterating various results with each other we are able to build out a total graphical picture.

We also can use the data that we develop in Maltego to feed our i2 link analyzer. This lets us correlate the information we got from Intel 471 and perform some sophisticated analysis on it in the context of the rest of our findings.

We could not do our threat research without it. Every malware, attack, campaign and other indicator has a human actor. Intel 471 lets us identify and track those actors and their acts. We designate Intel 471 SC Lab Approved for another year. – *Peter Stephenson, technology editor*

SC MEDIA LAB APPROVED *One year later*

DETAILS

Product Actor-centric intelligence collection

Company Intel 471

Price Contact vendor.

What it does Actor-centric cyberthreat intelligence collection focused on closed source intelligence collection of financially motivated cybercriminals and hacktivists.

What we liked The ease of use and power of its searches, plus the immense actor database and ease of setting up "watchers" to flag activity by selected actors.

The bottom line If you are doing any sort of cyberthreat intelligence, you need to monitor the Dark Web. This tool, without question, is the way to do that.

Events Seminars

Start here for a calendar of events.
To have your event included, contact scfeedbackUS@haymarketmedia.com

FEBRUARY

» RSA Conference 2017
Feb. 13-17
Take advantage of this opportunity to learn about new approaches to info security, discover the latest technology and interact with top security leaders and pioneers. Hands-on sessions, keynotes and informal gatherings allow you to tap into a smart, forward-thinking global community that will inspire and empower you.
Venue: San Francisco
Contact: rsaconference.com

» SC Awards 2017
Feb. 14
The mission of the SC Awards is to honor the achievements of companies and information security professionals striving to safeguard businesses, their customers and critical data in North America. Competitors are voted on by two panels of judges comprised of a range of cybersecurity industry luminaries – from current and former CISOs to vendor-neutral consultants or analysts to educators from academic institutions – all members of SC's audience. Results are completely independent. Financial/advertising considerations play no part in the results.
Venue: San Francisco
Contact: scmagazine.com/awards

» SANS Dallas 2017
Feb. 27-March 4
Information security training in Texas from SANS Institute, with a course line-up including core fundamentals, penetration testing, digital forensics, and security management.
Venue: Dallas
Contact: sans.org/event

SC CONGRESS LONDON

»SC Congress London
Feb. 23
As a continuation of SC Media's outstanding news coverage and latest cyber-security solutions, we present our fifth installment of SC Congress London, a destination for analysis on all of the latest cybersecurity issues. Our curated topics and speakers are chosen to guide and educate our fellow U.K. cybersecurity practitioners with the knowledge they need for tomorrow, including an opening keynote from the senior director at the NCSC. This year at SC Congress London we will also be showcasing our new format, which includes new technical editorial tracks exploring ransomware, data breaches and DDoS protection.
Venue: ILEC Conference Center, London
Contact: sccongress.com/london

MARCH

» Cyber Security Summit Denver
March 1
The Cyber Security Summit is an exclusive C-Suite conference series that connects senior level executives responsible for protecting their companies' critical infrastructures with innovative solution providers and renowned information security experts. This educational and informational forum will focus on educating attendees on how to best protect highly vulnerable business applications and critical infrastructure. Attendees will have the opportunity to meet the nation's leading solution providers and discover the latest products and services for enterprise cyber defense.
Venue: Denver
Contact: cybersummitusa.com

» Black Hat Asia 2017
March 28-31
Black Hat is returning to Asia again and has quite an event in store. Hear the brightest professionals and researchers in the industry who will come together for four days--two days of deeply technical hands-on trainings, followed by two days of the latest research and vulnerability disclosures at briefings.
Venue: Singapore
Contact: blackhat.com

» Women in Cybersecurity
March 31-April 1
In spite of the growing demand and tremendous chances in the job market, cybersecurity remains an area where there is lack of skilled professionals nationally, regionally and internationally. Even worse, women's representation in this male ruled field of security is low. Through the WiCyS community and exercises, expect to raise awareness about the significance and nature of the cybersecurity profession.
Venue: Tucson, Ariz.
Contact: csc.tntech.edu/wicys

APRIL

» SANS Threat Hunting and IR Summit 2017
April 18-25
The Threat Hunting & Incident Response Summit will focus on specific hunting and IR techniques that can be used to identify, contain and eliminate adversaries targeting your networks. Visitors will have the opportunity to directly learn from and collaborate with IR and detection experts who are uncovering and stopping the most recent, sophisticated and dangerous attacks against organizations.
Venue: New Orleans
Contact: sans.org/event

JULY

» Black Hat USA 2017
July 22-27
Black Hat – built by and for the global information security community – returns to Las Vegas for its 20th year. This six-day event begins with four days of intense trainings for security practitioners of all levels followed by the two-day main event, including more than 100 independently selected independent and sponsored briefings and sessions, a CISO Summit, a business hall, arsenal, Pwnie Awards, and more.
Venue: Las Vegas
Contact: blackhat.com

ADVERTISER INDEX

Company	Page	URL
Privoro	13	https://privoro.com
RiskSec	Inside front cover	risksecny.com
SC Awards	Back cover	scmagazine.com/awards
SC Media	23	scmagazine.com
SC Virtual	15	scmagazine.com
SC Subscription	Inside back cover	www.scmagazine.com/requal

Many targets for one email attack

Deploying a multi-layered email security setup is crucial, says Mimecast COO Ed Jennings.

Supply chains are relationships of convenience and mutual benefit for businesses working together. But, today, those relationships have turned those businesses into prime targets for cybercriminals. Their M.O. is simple: breach one company in a supply chain, with fewer IT resources and less awareness about cybersecurity needs, then use that breach to pivot to even bigger fish in the same pond. Cybercriminals will target enterprises that might be more prepared against an attack on their front door, but are less suspecting of one coming through the backdoor, under the guise of one of their partners.

Considering 70 percent of cyberattacks involve a secondary target after the first strike, it's easy to see how a breach at one supply chain partner can quickly bleed over to several others – without anyone realizing, until it's too late.

#1 attack vector: Email

Over 90 percent of cyberattacks happen through email. In just one three-month period, more than half of organizations reported an increase in whaling attacks: malicious emails that deceive recipients into opening them by mimicking the credentials of executives like a CEO or CFO. This is even more problematic in the supply chain where whaling attackers can pretend to be an executive at a company's partner to ask for access, making it easier for the thief to pass themselves off as genuine.

Email is the number one attack vector for businesses today. But, many alternatives proposed for managing email threats – web portals, email encryption or file sharing – are too cumbersome for employees to bother with. After all, email is so ubiquitous because it's quick and easy to use. Having additional hoops to jump through makes sharing information a chore, and one that supply chain partners could ignore in favor of email, in spite of its vulnerabilities.

Shielding yourself

You don't want to deny employees email as a communications tool. But, you also have to ensure everyone is keenly aware of the threats surrounding that channel. That's why the key to cybersecurity in the supply chain is to build a human firewall. It encompasses the best of both worlds: employees throughout the supply chain continue to use email, but share a foundation of awareness and information about the telltale signs of an email attack, like spear phishing or whaling. The more everyone is informed about what email attacks truly look like, the less likely they are to fall for one.

Deploying a sophisticated, multi-layered email security setup is also crucial for defending against email vulnerabilities. Building in that level of redundancy provides greater oversight of the messages, links, attachments or spoofed domain names that may be coming into someone's inbox – and flags them before an unsuspecting employee opens a Pandora's box on the supply chain.

> "...the key to cybersecurity in the supply chain is to build a human firewall."

Strong as its weakest link

Supply chain partners don't just share the same successes, they share the same risks, too. Any company within a supply chain has to prioritize and implement its own cybersecurity protections. Whether it's building up a human firewall of awareness or integrating a multi-layered email security system to catch threats before they come through the door, the more one partner reduces their vulnerability, the more it protects everyone in the supply chain. Otherwise, everyone is at risk, regardless of what other steps they may be taking individually.

Don't be the weak link in your supply chain. Protect yourself the way you expect and need your partners to protect themselves.

Ed Jennings is chief operating officer at Mimecast, a cloud-based email management firm.