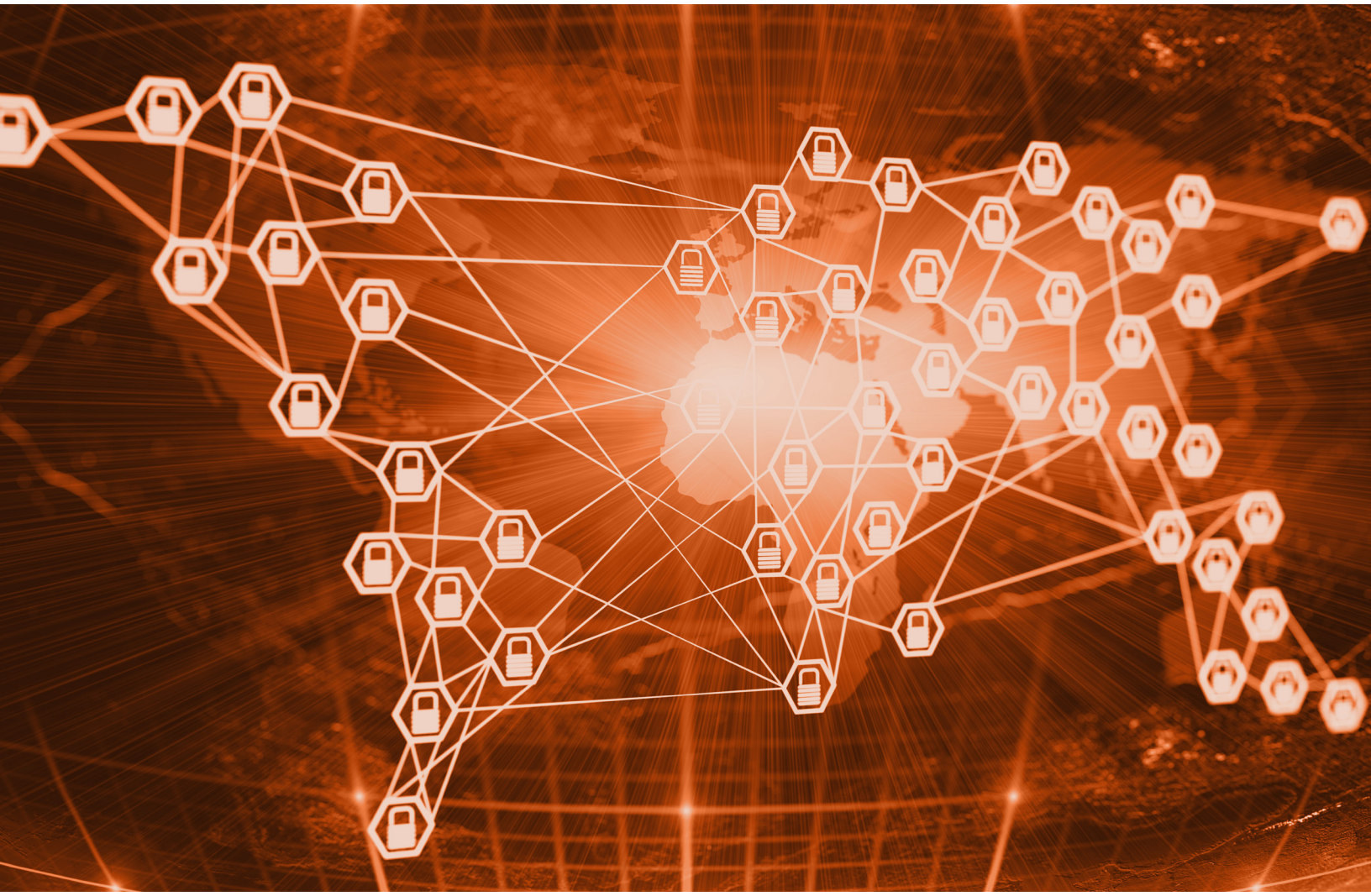
RETHINKING THE APPROACH TO CYBERSECURITY

How Enterprise Security Leaders are Now Forced to Address Top Security Threats



The cyberthreat landscape continues to grow and evolve. Cybersecurity Ventures predicts that cybersecurity will become a $1 trillion enterprise between 2017 and 2021.[1] What is more frightening is the fact that the cost of cybercrime is projected to tally to over $6 trillion during the same timeframe.

Despite new and evolved cybersecurity technologies, IT professionals lack confidence. Seventy-five percent of them feared they would fall prey to cyberattacks this past year—and there is no reason to think this percentage will decrease in 2017.[2] This makes sense considering that nearly half believe they can no longer identify malicious activity traversing their networks and 86 percent report their cybersecurity function does not meet organizational requirements.[3]

Part of the challenge is that the digital footprint of organizations continues to expand. For example, the amount of data being generated doubles every two years.[4] Protecting all of this data—at rest and in transit—is a significant challenge. The surface of corporate networks is expanding rapidly, too. New devices are being introduced while existing devices that were previously unconnected to the network are being connected. Add that employees use an average of three-plus devices for work activities daily, including 40 percent of companies reporting that they have a BYOD policy in place, and the threat landscape becomes even more menacing.[5]

In a recent white paper, Fortinet identified five cyberthreat areas that are putting organizations at risk today:[6]

- Cloud Adoption
- Internet of Things
- Ransomware
- Secure Sockets Layer (SSL) Encryption
- Shortage of Cybersecurity Professionals

CLOUD SECURITY

ADOPTION OF THE CLOUD

Despite all of the fanfare and discussion around cloud computing, it still comprises less than 15 percent of total IT spend. What this means is that the majority of cloud adoption is still ahead of us. The global cloud market is growing at an annual rate of 22 percent, topping $146 billion this year,[7] and it is forecast to exceed 50 percent of IT budgets by 2019.[8]

Regardless of the cloud model, service delivery modes vary, with most enterprises embracing a wide range of services: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). A new wave of adoption is certainly on the way: by 2020, 92 percent of workloads will be processed in the cloud versus 8 percent by traditional data centers.[9]

The cloud splits out into public, private, and hybrid offerings. Research shows the public cloud is growing faster than the private cloud, with 68 percent of cloud workloads predicted to be in public clouds by 2020 (up from 49 percent last year). Much of this is tied to the adoption of SaaS-based applications, which substantially increases the amount of data being stored in the public cloud as well as the amount of data being exchanged between different applications and systems.

REASONS DRIVING CLOUD ADOPTION

So, what is driving all of this cloud adoption? Enterprise leaders cite the following as the most predominant factors:[12]

- Availability, 46%
- Cost Reduction, 41%
- Flexible Scalability, 36%
- Reduced Complexity, 14%
- Regulatory Compliance, 13%

The aggregate outtake from each of these is that businesses can compete more effectively by tapping the opportunities of the cloud. And as the cloud becomes the new normal, many businesses that do not embrace the cloud will find themselves unable to compete.

CLOUD SECURITY CONCERNS

Managing security and compliance across these disparate cloud services—whether public, private, or hybrid—is a challenge. Ironically, even though 64 percent of IT professionals believe the cloud is more secure than on-premise infrastructure security, they concurrently list security as their most prevalent challenge when it comes to the cloud.[13]

Further adoption of SaaS-based applications and transmission of data to and from the cloud rank at the top of the list of concerns. But there are other factors ratcheting up security anxieties. As the number of SaaS-based applications grow, so do the interdependencies between them.

3/4 of IT professionals fear their organizations will become a victim of a **cybersecurity attack** in the next year

86% of IT professionals believe their cybersecurity function does **not** meet the requirements of their business

DATA STORED IN CLOUD[10]

- Email, 44%
- Customer Data, 32%
- Sales and Marketing Data, 31%
- Employee Data, 30%
- Contracts, Invoices, Orders, 26%
- Financial Corporate, 19%
- Intellectual Property, 18%

BUSY BUILDING CLOUDS[11]

Percentage of IT leaders who report they are building …

- Public Clouds, 32%
- Private Clouds, 38%
- Hybrid Clouds, 59%

SECURITY BARRIERS TO CLOUD ADOPTION[15]

- Security Concerns, 53% (up from 45% last year)
- Regulatory Compliance, 42% (up from 29% last year)
- Data Loss Risks, 40%

DevOps, which seeks to integrate "development, IT operations, security, and quality assurance under a single automated umbrella," introduces both new security challenges and opportunities. With much of DevOps happening in the cloud, organizations must find new ways to integrate security into the continuous loop of planning, coding, testing, deploying, operating, and monitoring.[14]

IoT

IoT GROWTH[16]

The Internet of Things (IoT) is growing in leaps and bounds. Many industry segments are seeing the number of IoT devices connected to the network grow 50 percent annually. Projected forecasts are almost mind-numbing. IHS predicts the IoT market will double to 30.7 billion devices by 2020—and 75.4 billion by 2025![17] Revenue forecasts are equally impressive, with estimates of $300 billion by 2020 and a global economic impact of $1.9 trillion.[18]

For certain industry segments, IoT devices are transformative. Consider healthcare as an example, where IoT devices are able to deliver better patient care while improving efficiencies. Doctors can maintain real-time monitoring of patients when they are moved home. Transportation and distribution is another industry segment where IoT is making a big difference. Shipping companies can track everything from vehicle fuel and consumption to monitor and control shipping containers.

SECURITY CHALLENGES OF IoT

IoT devices have the potential to become more pervasive in the lives of people (consumer IoT) and businesses (industrial IoT) than smartphones. The security concerns are amplified because of the use cases for these IoT devices—both in terms of the data they transmit as well as the systems they access and control. And as IoT devices propagate, so will the security risks associated with them.

Malicious attacks on IoT devices are easier than with many other network connections, as they were not designed or built with security in mind—having weak authentication and authorization. Additionally, the vast majority of IoT devices are "headless," meaning traditional security software used to block malware cannot be installed on them.

Automotive IoT space is an area where significant growth and opportunity exists. It is predicted to grow at a 22 percent compound annual growth rate (CAGR) through 2025.[20] Yet, the proliferation of IoT-connected vehicles will offer cybercriminals a much larger attack surface, and there are catastrophic possibilities.[21]

Some IoT hacking of "intelligent" vehicles may simply cost time and money, such as a ransomware attack demanding payment in exchange for unlocking a vehicle or reactivating an entertainment or navigation system or the theft of confidential personal information. In other instances, the consequences may be much more dire, such as the loss of control of brakes, engines, or steering that result in serious life-threatening accidents.

For individuals, IoT devices have access to personal information related to health, finances, education, home, and more. For businesses, IoT devices have access to manufacturing and supply chain operations, healthcare systems, critical infrastructure, and other systems. A malicious compromise in these systems can incur substantial ramifications. Individuals can lose highly confidential personal information, while businesses can experience system outages due to a denial-of-service attack and data loss. In certain instances, critical infrastructure failure of supervisory control and data acquisition (SCADA) systems that monitor and control dams, transportation systems, food supplies, and electrical grids could not only cost millions of dollars but also put lives at risk.[22]

MOST PREVALENT SAAS APPS

Currently Deployed	SaaS Application	Plan to Deploy
41%	Microsoft Office 365	20%
27%	Salesforce	7%
24%	Microsoft Exchange	11%
20%	Google Apps	6%
17%	Dropbox	5%
15%	ServiceNow	5%
14%	Box	4%
9%	Workday	4%
8%	None	5%
7%	SuccessFactors	3%

IoT INDUSTRY GROWTH[19]

- Energy and Utilities, 58%
- Home Monitoring, 50%
- Transportation and Distribution, 49%
- Smart Municipalities (Government), 43%
- Agriculture, 33%
- Healthcare and Pharmaceuticals, 26%

IoT SECURITY RISKS[23]

1. *Security Vulnerabilities*. Devices shipped with software that is outdated or becomes outdated over time.
2. *Unsure Communications*. Unencrypted communications and data leaks.
3. *Data Leaks*. These can occur both between devices and from the cloud.
4. *Malware Infection*. Malware can infiltrate IoT devices and disrupt their operations and compromise their data.
5. *Service Disruption*. Loss of availability or connectivity may degrade the security of devices and expose systems such as home alarm systems, putting them at risk.

RANSOMWARE

Ransomware attacks more than doubled last year, with upwards of 4,000 attacks occurring daily that infected an average of 30,000 to 50,000 devices each month. The amount of ransom paid last year increased thirty-fivefold—skyrocketing from $24 million to $850 million. Ransom demands also expanded—jumping from an average of $294 in 2015 to $679 last year. And with fewer than one-quarter of organizations reporting ransomware attacks, these numbers likely are substantially higher.[24]

Ransomware attacks are also morphing and becoming more automated due to the availability and affordability of automated malware services such as ransomware as a service, botnet rentals, and spearphishing services. In addition, traditional ransomware typically went after an organization's data, encrypting and locking the files until the ransom was paid. But with the emergence of IoT, a new strain has developed that targets control systems powering vehicles, assembly lines, and power systems. It locks the underlying boot system, thus rendering the devices inoperable without an option to restore them from backups or a decision by the owner to pay the ransom.

The impact of ransomware is not only in the ransom being paid but also the repercussions to business operations. Downtime can translate into financial losses, environmental impact, or even the loss of human life. For example, last year, 63 percent of businesses reported that a ransomware attack led to operational downtime. Forty-eight percent indicate it led to the loss of hardware or data.[25] And with high-value, confidential data often being hacked, cybercriminals are increasingly threatening the release of the information.

DISTRIBUTION OF RANSOMWARE[26]

- Email Links, 31%
- Email Attachments, 28%
- Website Attachments, 24%
- Unknown Sources, 9%
- Social Media, 4%
- Business Applications, 1%

SSL ENCRYPTION

SSL TRAFFIC ON THE RISE

SSL traffic accounts for anywhere between 35 and 50 percent of network traffic today,[27] and it continues to grow at a clip of 20 percent annually.[28] Websites are increasingly implementing HTTPS by default, though much work remains on this front. As those websites adopt HTTPS, the overall percentage of SSL traffic will grow.[29] Cloud adoption is another reason for the increase, as organizations seek to protect their data in transit to and from the cloud. SaaS applications like Salesforce, Dropbox, and Microsoft Office 365 have taken privacy to heart and enabled SSL encryption on their platforms.

Organizations across various industry segments must encrypt certain types of sensitive data in transit using Secure Sockets Layer (SSL) encryption to remain in compliance with regulations such as PCI-DSS (Payment Card Industry Data Security Standard) and HIPAA (Health Information Portability and Accountability Act).

CHALLENGES OF SSL ENCRYPTION

Yet, SSL encryption is a double-edged sword. Cybercriminals used to hide their malware and ransomware from traditional security solutions, slipping past enterprise defenses. In addition, they also use SSL encryption to encrypt their communications with command and control systems. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are trained to trust encrypted traffic, and thus unable to detect ransomware. The growing number and complexity of ciphers for encryption by good and bad actors necessitates the need for decryption. As cybercriminals typically employ the most advanced ciphers when encrypting their malware, there is a heightened need to support industry-mandated ciphers for such decryption.

So, what is the result? Ninety percent of CIOs indicate they have experienced or experience a network attack using SSL encryption, and 87 percent say their security defenses are less effective today due to cybercriminals using encryption to hide their attacks.[30]

SSL encryption can also impact network performance while increasing the complexity of managing network security. SSL decryption and traffic inspection systems can increase network latency and even disrupt business operations. Additionally, SSl encryption can increase the complexity of managing network security by introducing additional hardware and software as well as security policies and workflows.

But there are ways to avoid performance compromises. For example, one of the ways to avoid compromises to network performance is to conduct SSL encryption with threat-prevention features. This enables organizations to decrypt and identify whether clear text is malware without impacting performance.

SHORTAGE OF CYBERSECURITY PROFESSIONALS

The growing complexity of managing security is a problem for many organizations. Nearly 40 percent of enterprises indicate they have five-plus security solutions.[31] The difficulty of managing this patchwork of solutions is ratcheted up each time an additional point solution is overlaid on top of it. One result is that 40 percent of organizations are opting not to upgrade their networks.[32]

WHERE TO USE SSL DECRYPTION AND INSPECTION

- Email
- Web Browsing (Website and Social Networks)
- SaaS Applications
- Custom Business Applications

HOW CYBERCRIMINALS USE SSL ENCRYPTION

1. *Hiding the Initial Infection.* Cybercriminals encrypt their malware and send it through an approved port; users click on embedded links that take them to sites containing the payload or as an attached file. One example of this type of attack is Heartbleed, a security bug in the OpenSSL cryptography library used widely for the implementation of SSL. It is able to hack and infect systems through a server or a client and results from improper validation in the implementation of the Transport Layer Security (TLS) heartbeat extension.
2. *Hiding Command and Control.* Certain malware families use encryption to hide command and control communications.
3. *Hiding Data Exfiltration.* Many malware families also use encryption to hide network information such as passwords and stolen information (e.g., bank accounts, passwords).

Finding IT security professionals with the knowledge and experience to implement and manage these solutions is a difficult task. Here is the catch: there is a shortage of IT security professionals, with estimates in the range of one million more who are needed today. And despite many corporate boards recognizing the importance of security and mandating educational initiatives to train more IT security workers, the projection is the shortage will continue to grow—reaching 1.5 million globally by 2020.[33]

IT leaders know there is a problem: nearly two-thirds list IT security as the top skillset on their teams for which to recruit (the next highest is software development at 18 percent).[34] Three-quarters believe they will face more security threats in the next five years due to a shortage of IT security talent. Over half place recruiting IT security professionals with specialized skills or expertise on their list of top priorities.[35]

All of these factors translate into an impact to the business. Over half of IT leaders indicate a shortage of cybersecurity staff has increased the workload on existing staff, 35 percent have compromised on filling roles with the right skill sets and experience, and another 35 percent say their teams have been unable to learn or fully utilize all of their security technologies. Even more frightening is the revelation that over half disclose their organizations experienced at least one cybersecurity event that can be tied back to the lack of security training and staff resources.[36]

Most in Demand	Most Challenging to Find
Cloud Security, 51%	Cloud Security, 32%
IT Security Technologies, 47%	IT Security Technologies, 29%
Big Data/Data Analytics, 37%	Security Architecture, 26%
Applications Security, 30%	Hacking/Penetration Testing, 26%
Hacking/ Penetration Testing, 30%	Applications Security, 22%

CYBERSECURITY SKILLS SHORTAGE

The compound annual growth rate (CAGR) for IT security talent is around 10 percent, whereas the growth in the number of new IT security professionals is only a 5.6 percent CAGR.[38]

IT SECURITY STAFFING DISTRIBUTION[39]

- Use Only Full-Time Employees, 52%
- Use Only Contractors, 15%
- Use a Mix of FTE and Contractors, 33%

SORTING THROUGH YOUR SECURITY OPTIONS

Keeping pace with the continual evolution and advancements in the threat landscape is a difficult undertaking. The aforementioned five cybersecurity areas present IT security leaders with a steep climb when it comes to protecting their networks and data.

Enterprises have three overarching security architecture choices:

POINT SECURITY SOLUTIONS

The first is to acquire point solutions that address specific cybersecurity requirements. But with the evolution and changes in cybersecurity, this model is fraught with inefficiencies, gaps, and even deficiencies.[40] The following are some of the challenges associated with point solutions:

1. Management and Staffing

Implementing and administering each of the point solutions becomes a task in isolation from each of the other point solutions. And with nearly 50 percent of enterprises indicating they have five or more security solutions in place, this can quickly become a substantial undertaking—incurring a substantial impact on an organization's cybersecurity staff (from finding, recruiting, and retaining the right staff to keeping staff trained on each of the different solutions).

2. Disaggregated Policy Management

It is difficult to integrate disparate point solutions and get them to communicate with one another. Further, IT organizations cannot develop universal policies used to manage security across each of them, but rather must create policies unique to each point solution and manage each set separately. Not only is this inefficient, but it also creates security gaps that cybercriminals can exploit.

3. Lack of Integration

Integrating each of the point solutions is a time-consuming task that is never complete. Additionally, it is difficult—and sometimes impossible—to integrate each of the point solutions with other third-party technologies. And each time a new point solution is introduced, IT staff must retrace their earlier integration steps.

4. Visibility in Silos

With point solutions, IT security teams are unable to see across their entire enterprise. Each point solution has visibility, but only in their individual silos. Once again, this creates inefficiencies, as well as potential security weaknesses.

5. Myopic Intelligence

A robust cybersecurity environment leverages all of the different pieces to construct a much stronger whole. However, IT security teams cannot share threat intelligence across different point solutions and lack a holistic view of intelligence and moreover collaborative intelligence sharing across the entirety of the attack surface.

6. Performance

Point solutions run on hardware—either on proprietary appliances or servers—which is based on off-the-shelf processors that lack high-performance computing capabilities. This creates performance processing logjams as well as sluggish networks and applications, all of which impact end-user productivity and operational efficiencies.

SECURITY PLATFORMS

The number of entry points is dramatically larger today than it was just a few years ago. Enterprises must protect themselves at dozens or even hundreds of different entry points resulting from the use of cloud services, various devices, and mobile workers. Security is much more than just protecting the perimeter; organizations must also protect their data centers, branch offices, cloud applications, and partner locations, among others.

Platform solutions arose to meet this proliferating cybersecurity landscape. But due to the fact that they have their roots in one specific security element, such as security firewalls or endpoint security, the additional components these providers bolt onto their platforms become a collection of tools rather than a seamless fabric.[41] The following are some of the disadvantages of platform solutions:

1. Centralized Console

Security platforms connect each of the different elements within the platform through a centralized management console. But this results in time delays that slow communications and collaboration between the different components in the platform, thus impacting an organization's ability to respond to threats such as zero-day attacks.

2. Performance

The same performance problems that exist with point solutions also plague platform solutions. The appliance-based hardware for platforms is based on off-the-shelf processors that are not designed for the unique requirements of cybersecurity. Organizations often need to purchase additional equipment—running on off-the-shelf processors—from the security platform provider to achieve the level of performance necessitated by their business requirements.

3. Scale and Agility

Cybersecurity is a fast-changing, dynamic environment. Platform solutions can scale to meet new requirements by either replacing existing equipment with newer, higher-performing ones or by adding more devices and equipment. But this incurs additional costs and is too slow to address spikes in network traffic and the emergence of new cyberthreats, among other issues.

4. Security Blind Spots and Gaps

Whenever multiple products are combined underneath one umbrella, there are bound to be gaps and blind spots—whether related to integration or missing capabilities. Cybercriminals can take advantage of these to infiltrate your network. With the growth in IoT devices and the use of SSL encryption to conceal inbound and outbound threats, the potential for these security gaps and blind spots increases. Platform solutions, with their bolted additions, lack the agility and breadth of integration and automation to thwart these threats.

5. Missing Visibility

The different products comprising a platform solution likely have different dashboards, means for collecting data, and reporting mechanisms. Some attempt to aggregate this information manually, but doing so is a time-consuming effort and is certainly not done in real time. And without transparent, real-time visibility across its entire network, an enterprise lacks the intelligence needed to make proactive cybersecurity decisions, something particularly important where zero-day attacks are increasingly the norm.

6. Third-Party Integration

Individual products in the security platform often have their own APIs and interfaces, making it difficult to connect and integrate third-party solutions. Suddenly, enterprises find themselves facing some of the same silo-based challenges as those using point solutions.

SECURITY FABRIC

A new alternative to point and platform solutions is a security fabric. All security solutions within the fabric are made available to all other points in the environment in real time—from IoT devices to the cloud. The following are some of the key outcomes of a security fabric:

1. Real-Time Communications

The security fabric seamlessly integrates each of the different pieces within the environment, while also enabling IT organizations to add third-party products to the fabric. Each of these communicates in real time with each other, helping to facilitate collaborative intelligence.

2. Entire Attack Surface Covered

Unlike point solutions that cover only a portion of the attack surface, the security fabric is all-encompassing. Its coverage includes the cloud, applications, network, access points, endpoints, and IoT devices. This translates into transparent visibility and a more robust threat posture.

3. Performance and Infrastructure Impact

Whereas point and platform solutions use off-the-shelf processors, the security fabric leverages advanced security processors designed specifically for the demands of cybersecurity. The security fabric also includes hardware-based parallel path processing that increases throughput performance while enabling scale during influxes of SSL-encrypted traffic. Robust whitelisting enables organizations to push known traffic while focusing processing resources on unknown threats.

4. Automated, Dynamic Responses

The security fabric includes technologies that allow it to identify known and unknown threats using technologies such as whitelisting and sandboxing. This "integrated whole" responds to threats and attacks in a fully coordinated manner between each of the solutions contained within the security fabric.

FIVE SECURITY FABRIC TAKEAWAYS

So, recognizing the benefits of the security fabric over traditional point solutions and platform solutions, how might the security fabric benefit each of the five emerging cybersecurity threats that were identified?

CLOUD

The emergence of the cloud requires organizations to add additional point solutions and for platform providers to bolt new solutions onto their platforms. But this creates integration challenges, incurs substantial staff requirements, and leaves gaps and blind spots into and around which cybercriminals can sneak through. The security fabric is a better option, weaving cloud applications into its broader environment governed by universal security and compliance policies and managed via transparent visibility across the entire attack surface.

IoT

The rapid growth in IoT devices creates highly pernicious threats. The ability to seamlessly add them to the security fabric gives organizations greater agility while mitigating potential threats. For enterprises relying on point solutions, they likely need to add another point solution to protect their IoT devices. In the case of platform solutions, enterprises may need to have the provider bolt additional components onto the platform before they can be protected.

Because IoT devices are deployed pervasively, it is difficult to create transparent visibility and management across all of them. Many point and platform solutions are simply incapable of integrating all of them into a centralized management view, including access control and response. Likewise, scale—as more IoT devices are brought online—becomes an issue for point and platform solutions. In contrast, a security fabric can integrate all of the disparate access points of a network (endpoints, applications, the cloud, and IoT devices), regardless of their distribution, into an end-to-end solution that covers all of the different attack surfaces.

RANSOMWARE

Enterprises wishing to thwart ransomware attacks require a security fabric that covers the different delivery channels cybercriminals employ to gain entry—email links and attachments, website attachments, business applications, social media, and even IoT devices. Just as IT organizations must remain vigilant for inbound threats, the same must be said about outbound threats. Here, enterprises using a security fabric can also monitor outbound communications for ransomware-encrypted command and control communications as well as hacked files locked with private-key encryption. The security fabric uses automated local threat intelligence sharing to disrupt command and control communications, the lateral spread of infections, and at patient zero (before it spreads to other users and endpoints).

SSL ENCRYPTION

SSL encryption is an important tool in the IT security toolbox, enabling enterprises to protect highly sensitive and confidential information. Unfortunately, it is also a critical tool in the toolbox of cybercriminals, who use encryption to gain entry and then conceal their theft of information or ransomware hacking. Unlike point and platform solutions, a security fabric is able to deliver highly integrated and high-performance SSL decryption and inspection processes—for both inbound and outbound communications across the entirety of the attack spectrum.

CYBERSECURITY STAFFING SHORTAGES

Cybersecurity professionals are in short supply and enterprises are limited in terms of the number of IT security professionals they can hire. With the number and virulence of cyberthreats growing and the complexity of security architectures increasing, the security fabric is a compelling alternative to point and platform solutions that require cybersecurity staff trained and well-versed on multiple product and solution components. Specifically, all aspects of security are intertwined in a security fabric for a centralized and transparent view, helping enterprises to avoid hiring IT security specialists and giving existing cybersecurity staff to scale in their support of an ever-growing and evolving security landscape.

[1] "Cybersecurity Market Report," Cybersecurity Ventures, December 2016.

[2] "The State of Cybersecurity: Implications for 2016," ISACA and RSA, February 2016.

[3] "Path to Cyber Resilience: Sense, Resist, React," 19th Global Information Security Survey, EY, December 2016.

[4] "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," IDC, April 2014.

[5] "BYOD and Mobile Security," Crowd Research Partners, 2016.

[6] "A Security Leader's Definitive Guide to the Threat Landscape," Fortinet, February 2017.

[7] Clint Boulton, "6 Trends That Will Shape Cloud Computing in 2017," CIO.com, November 2, 2016.

[8] Fredric Paul, "Cloud to Consume Almost Half of IT Infrastructure Sales by 2019," Network World, July 7, 2015.

[9] Joe McKendrick, "With Internet of Things and Big Data, 92% of Everything We Do Will Be in the Cloud," Forbes, November 13, 2016.

[10] "Cloud Security: 2016 Spotlight Report," LinkedIn Security Group, 2016.

[11] Ibid.

[12] "Cloud Security: 2016 Spotlight Report," LinkedIn Security Group, 2016.

[13] Sarah Patrick, "Security and the Cloud: Trends in Enterprise Cloud Computing," Clutch, March 3, 2016.

[14] Doug Drinkwater, "Is DevOps the Holy Grail for Information Security?" CSO.com, March 4, 2016.

[15] "Security and the Cloud," Clutch.

[16] "Cloud Security: 2016 Spotlight Report."

[17] Louis Columbus, "Roundup of Internet of Things Forecasts and Market Estimates, 2016," Forbes.com, November 27, 2016.

[18] Gil Press, "Internet of Things by the Numbers: Market Estimates and Forecasts," Forbes, August 22, 2014.

[19] "State of the Market: Internet of Things 2016: Accelerating Innovation, Productivity, and Value," Verizon, December 2016.

[20] Andrew Meola, "Automotive Industry Trends: IoT Connected Smart Cars & Vehicles," Business Insider, December 20, 2016.

[21] "Motor Vehicles Increasingly Vulnerable to Remote Exploits," Federal Bureau of Investigation, March 16, 2016.

[22] Ed Nugent, "SCADA Cybersecurity in the Age of the Internet of Things," Control Engineering, August 30, 2016.

[23] "Internet of Things (IoT) Security and Privacy Recommendations," BITAG, November 2016.

[24] Minal Khatri, "Ransomware Statistics – Growth of Ransomware in 2016," Systweak, August 25, 2016.

[25] "State of the Channel Ransomware Report 2016," Datto, 2016.

[26] "Non-Malware Attacks and Ransomware Take Center Stage in 2016," Carbon Black Threat Report, 2016.

[27] See, e.g., J. Michael Butler, "SANS Institute InfoSec Reading Room: Finding Hidden Threats by Decrypting SSL," November 2013; Johnnie Konstantas, "SSL Encryption: Keep Your Head in the Game," Security Week, March 15, 2016.

[28] Butler, "SANS Institute InfoSec."

[29] Brian Barrett, "Most Top Websites Still Don't Use a Basic Security Feature," WIRED, March 17, 2016.

[30] Jai Vijayan, "When Encryption Becomes the Enemy's Best Friend," Dark Reading, March 5, 2016.

[31] "Top Networking and Security Challenges in the Enterprise: Planned Network Investments in 2017," Global Industry Report, CATO, November 2016.

[32] "Protecting Your Organization in a Talent-Scare Market: Information Security," Experis, 2015.

[33] Michael Suby, et al., "The 2015 (ISC)2 Global Information Security Workforce Study," Frost & Sullivan, 2015.

[34] "Emerging Cyberthreats Report 2016," Georgia Tech Cyber Security Summit, Institute for Information Security & Privacy, 2016.

[35] Suby, "The 2015 (ICS)2 Global Information Security Workforce Study."

[36] Jon Oltsik, "Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II)," ESG and ISSA, December 2016.

[37] "Cybersecurity: Protecting Your Future, Early Adopters Win," Robert Half, 2016.

[38] "Protecting Your Organization in a Talent-Scare Market: Information Security," Experis, 2015.

[39] "Protecting Your Organization," Experis.

[40] Francisco Ordillano, "Security Fabric, Expertly Tailored to Fit Your Organisation," InfosecPartners, September 14, 2016.

[41] Zeus Kerravala, "Cybersecurity Fabric vs. a Security Platform: Fabric Wins," Network World, November 16, 2016.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

Feb 15, 2017
58160-A-0-EN