FORTINET

WHITE PAPER

Charting A New Course—The Holistic View Of Threats and Security Operations

Despite best efforts to protect networking environments, the occurrence of breaches is on the rise. The Identity Theft Researc Center (ITRC), which tracks and reports on all reported breaches throughout each year, measured a 40% increase year over year. They define a data breach as an incident in which an individual's name plus a Social Security number, driver's license number, medical record, or financial record (credit and debit cards included) are potentially put at risk of exposure. This exposure can occur either electronically or in paper format. Their data has shown that even the most recognized and respected brands, across all industry types, experienced breaches. Another recurring trend is the inability of organizations to rapidly detect, isolate, and remediate threats. Most studies continue to show that detection of attacks, containment, and remediation efforts are measured in days – not hours or minutes. That leaves an enormous amount of time for black hats to exfiltrate your data. For example, in a recent Ponemon Institute study[1], it took, on average, 6.4 days to resolve a malware-based cyber attack in 2017, and that is up almost 15% from 5.6 days in 2016. The same study found resolving attacks from malicious insiders took an average of 50.0 days in 2017 and attacks from malicious code took an average of 55.2 days!

It is no secret that the threat landscape today is markedly different than just a few short years ago, and it continues to morph and change at a rapid pace. Optiv[2] reports that organizations saw less than 1,000 security alerts in 2007, but by 2017, an average day for the same organization would see over 1,000,000 alerts. Moreover, we are in an environment where workers today expect to be able to conduct their business from any device of their choosing, in the location most conducive to personal productivity, and with applications that are not always tied to the corporate network. This shift of control from the technology provider to the technology user has changed the way we work and has created a whole host of challenges for those tasked with protecting data and technology assets. Couple this with the move to digitization and increasingly connected network resources, and you've created a target-rich environment for potential hackers.

Attackers exploit this new world, taking advantage of not only the thousands of new points of entry into the network but also by preying on the lack of attention users exhibit in an instant gratification world. The edge of the network has become blurred with new endpoints including mobile devices, sensors, and IoT devices like cameras, cable boxes, and thermostats. What's the impact? It's difficult to protect a network as the infrastructure and use become more complex. This new world requires a new approach. The approach must be holistic and adaptive in its view, yet tactical in its deployment of technology. An approach that focuses on more than just technology, recognizing that hackers use social engineering to lift credentials from unsuspecting employees, gaining a free pass to the network. An approach that moves beyond deploying silos of point products, exposing the enterprise when threats dynamically shift to a different target. This comprehensive approach to security must be more than just a command center full of dashboards and firewalls.

The Complex Challenges Of The Technology Executive

Today's IT executives are more than just technologists. They are business leaders with a seat at the decision-making table. As technology evolves, technology-driven business models are becoming more prevalent. The largest taxi service in the world, for example, is a technology company—Uber. As technology becomes more core to the corporate mission, initiatives taken on by the IT organization are more intertwined with day-to-day operations. With this as the backdrop, C-level executives are more driven than ever to quickly adopt technologies that can be tied to revenue and profit, shedding the old image of IT purely as a cost center. But often in the additional complexity, security becomes an afterthought. As an example, SD-WAN is quickly taking hold of many branch networks. As IT organizations rush to cash in on less expensive networks at the branch, letting SD-WAN technology negotiate transmission quality issues with these less expensive alternatives, many organizations forget that going directly to the Internet from the branch cuts out much of the security branches had protecting them from the data center. It's imperative for the CISO to bring this conversation into the executive suite and create a holistic approach to security—one that places security concerns at the front end of the conversation and brings forward an approach to address people, process, and technology.

Digitization is a prime, but not the only, example of how the CISO and other IT executives must deliver this complex balance of business enablement and security. Take, for example, a hospital or healthcare network. Electronic medical records clearly improve the quality of care for patients. Onsite caregivers can take advantage of past diagnoses and reach out across the world for a consult on a new X-ray image. But that transformational service comes with risk and compliance concerns. Are the records protected in accordance with HIPAA guidelines? How secure is the network the images travel on? What is the risk versus reward analysis when a patient's images will

be stored on a network you don't manage? This example illustrates well both the technology and process issues CISOs and security practitioners face when protecting corporate assets. These same challenges apply to a financial institution enabling its customers to access assets from their mobile phone or a retail firm processing credit card transactions at the point of sale. In the complex and connected world, data is always in flight, and data in flight is always at risk.

Technology Drivers

New and emerging technologies also present opportunities and challenges. Cloud has shifted the way in which organizations consume and deploy technology assets. No longer is it a given that the data center is a building with the firm's name on it with dedicated hardware on a secure private network. Today, compute resources are shared between departments and often between companies over the Internet. Just as virtualization advocates overcame concerns over hardware consolidation, IT visionaries overcame the fear of the security issues of shared infrastructure and gave birth to the public cloud. But the fact remains, as business users deploy cloud technology for marketing and human resources applications, and IT leverages IaaS to react to the demands of rapid application deployment, connections beyond the corporate network have created exposures.

Driven and enabled by cloud and high-speed networking, mobility has redefined the definition of the network for many in IT. Now tablets, smartphones, and a whole host of devices, often referred to as the Internet of Things (IoT), are endpoints to be managed and protected. Loss of a device, theft, or the inherent dangers of public Wi-Fi requires vigilance as to both technology and policy, in a paradigm where a device connects both to the corporate network and an employee's Facebook account.

Emerging Threats

A variety of threats are putting pressure on IT to act with increasing vigilance and urgency as well. Ransomware has become a popular choice for hackers, increasing exponentially over the past several years. New, unprotected network endpoints have become subject to recruitment as botnet zombies, supporting Denial of Service (DoS) attacks against global web brands. Attackers even appear to increasingly hide malicious info in otherwise benign graphics (e.g., PNG) files (not usually inspected by security technology), with more firms seeing steganographic exploit kits (e.g., Sundown) than any other[3]. As if sophisticated software threats were not enough, it's still process and people issues such as password hygiene that pose some of the greatest threats. In fact, Verizon reports that the use of stolen credentials is still the number one attack method found in reported breache[4].

In addition to threats from the outside, CISOs must tackle threats to the network, which loom inside the organization. Half of all malware is delivered via email according to Verizon[5]. That often means the original malware payload is physically brought inside the network on laptops or other mobile devices, being downloaded outside and bypassing most of the perimeter security. And, as if protecting the network from wrongdoers wasn't enough, one of the most salient emerging threats is the lack of competent security professionals to staff the team. According to Enterprise Strategy Group, respondents ranked cyber security skills as their biggest gap for the sixth year in a row[6]. Security professionals are one of the most sought-after experts in IT today, and few CISOs would say they have enough people with the right skills to protect the firm.

Gaps In Visibility

The traditional approach to meeting these challenges has been to invest in highly specialized products, or "point solutions," each designed to monitor, protect, and respond to specific types of threats. But this has created a discontinuity in the way the enterprise can view security events and analytics. A recent survey by Network World has shown that enterprises have on average 32 different Security Solution Providers' products deployed in their network. Monitoring the network is done in a disjointed fashion with no common view of the complete picture. Each point product comes with its own unique and proprietary dashboard and similar reporting systems. Often each also requires specialized and highly trained personnel to monitor specific types of threats in isolation. Data continues to show a wide gap, and an inherent growing need, for personnel with the skills to operate in this environment. These deployments can also create unplanned complexities in the development and implementation of the policy and procedure changes required within the organization to make the technology effective.

Nowhere is this issue more prominent than in the divide between the Security Operations Center (SOC) and the Network Operations Center (NOC). While these centers operate on the same network, they often do not share their reporting data, and in the rare case where they do, they do not have the ability to automate correlation of the data. This lack of coordination creates gaps in both visibility of potential threats and in the organization's ability to respond.

The future holds even more challenges, as shown in a survey that Black Hat has done for the past few years. They asked attendees at their event, "Looking two years out, what concerns you most as a security professional?" The number one answer recently has been the same—the Internet of Things (IoT). This is a big concern because IoT brings with it unknown security risks, as many of these devices don't have security in mind when they are built, and there are few tools to help in monitoring and managing that type of risk.

Taking Action

Threats are only increasing. The digitized and connected world is the new playground for cyber con men, organized crime, sovereign combatants, and the pajama-clad troublemaker. CISOs cannot be viewed as barriers to moving quickly. To be successful in meeting these challenges, CISOs must grapple with and solve the four immutable laws of networking:

Reduce Complexity

The pace of change is not slowing. New demands will create the need to expand, optimize, and do more with network infrastructure. Without a transparent approach, where operations and security teams share information and work from a common map, they will continue to be burdened with a patchwork of products, policies, and siloed information. The edge of the network will continue to blur and advance with new technology. You may never have full control over the devices at the edge of the network. Understanding this new fact of life and incorporating it into your risk analysis and planning is critical to creating better strategies to address it. A transparent solution is critical to combat the complexity of disparate types and sources of data and to streamline the operations and effectiveness of managing risks and threats.

Increase Speed

Businesses demand speed. Customer needs and competitive options continue to drive new ways of doing business. Data analytics will drive decision-making, and transactions will drive revenue. Network security can't get in the way. When the network is compromised or the flow of business is impacted by security measures, the business loses money. Security infrastructure must not inhibit the speed of deploying new applications, and the network must be optimized for both performance and security without compromise. This requires tools that facilitate more rapid detection, isolation, and remediation of threats if organizations are to stay competitive. A more integrated approach to security operations is needed to allow the enterprise to move forward without compromise and without fear that new opportunities or change will create unforeseen exposures.

Adaptive Visibility

Identifying the potential threats and risks an organization faces is key to developing the right approaches to securing the network. The right security operations approach will include technologies capable of collecting the best, current, and relevant threat intelligence data not only from within the organization but across the globe and integrate new learnings from real-time threats. Organizations will need a more integrated and cross-platform, meshed approach where elements of the security infrastructure are highly connected and capable of sharing information. Visibility includes knowing where and when elements are attaching to the network, their current configurations, and the ability to see any changes to that environment. It also includes user activities as they create, change, store, and access the various assets that the business controls.

Automating Operations

With the shrinking availability of skilled cyber security personnel, organizations need to adopt solutions that facilitate automated, rapid response of the necessary countermeasures. This includes not only the automation of attack response but the streamlining of "normal" security and network operations as well. This is an area where many organizations are opting to outsource some or even all of those functions to Managed Security Service Providers (MSSPs). In fact, according to IDC's Worldwide Semiannual Security Spending Guide, spending on security services in 2017, inclusive of Managed Security Services, Integration Services, and Consulting Services, will reach $31.2B. The intelligent network should also enable rapid onboarding of new devices and the ability to configure them seamlessly. Policies should be centrally managed and quickly fold into the network and security operations framework both seamlessly and automatically.

The Way Forward

Security operations will continue to take center stage as we move into a fully digitized world. The cost of vigilance is high both in terms of investment and the exposures caused by lack of investment. High-profile breaches damage the corporate brand and directly impact revenue. Fines for noncompliance in regulated industries are harsh but pale in comparison to the lost revenue caused by a major security event. Organizations must spend in proportion to their exposure, but above all, they must align and rationalize investments to the appropriate threats.

The proper response is paramount to avoid costly incidents. The frequency and speed with which attacks are launched, and with which a defense must be mounted, means integrated automation has to be at the heart of countermeasures. Manual intervention and real-time analysis driven solely by staff cannot match the speed with which attackers strike and adapt.

Compounding this challenge is the sophistication of new attacks. Attackers learn, adapt, and overcome old defenses by employing new approaches and leveraging social engineering. Hackers can move from direct assaults to deploying Internet-enabled devices, creating a web of botnets simultaneously hitting a target on multiple fronts. Defenses must be intelligent enough to sense the shift and adjust.

Underpinning all of this is a human element. An understaffed security function and an employee population unaware of how to defend critical data will too easily fall prey to even straightforward phishing attacks. This could be an organization's biggest exposure. Talent must be recruited and cultivated, and programs must be put in place to ensure security professionals understand not only how to train employees to use effective password hygiene but also how to leverage sophisticated analytics to predict exposures.

Above all, CISOs must think beyond hot, new products purporting to address the latest threat. Siloed products widen the gap between discovery and remediation, and this is a problem that can be solved. Thoughtfully building process and workflows to cross the chasm between operations and security will make a meaningful impact in improving an organization's real security posture.

[1] Ponemon Institute – 2017 Cost of Cybercrime Study

[2] Optiv – The Cyber Security Mega Cycle Aftermath, 7 September 2017

[3] Fortinet – Threat Landscape Report Q4 2017

[4] Verizon Data Breach Report 2018, page 8

[5] Verizon Data Breach Report 2018, page 5

[6] ESG Annual IT Spending Intentions Research – 2017

September 14, 2019 6:29 AM

91843-A-0-EN

D:\Fortinet\White Paper\Charting a New Course\wp-FA-charting-a-new-course-the-holistic-view-of-threats-and-security-operations-teal\wp-charting-a-new-course-the-holistic-view-of-threats-and-security-operations-teal-V1