A SECURITY LEADER'S DEFINITIVE GUIDE TO THE THREAT LANDSCAPE

The transition to a digital economy is requiring networks to evolve rapidly. Applications, data, and services need to flow faster, and in growing volumes, across an increasingly diverse landscape of users, domains, and devices. Keeping up is only part of the challenge. The question that needs to be asked is, how do you balance this change and opportunity with risk? IoT and cloud-based applications, services, and infrastructures now require organizations to worry about an attack surface that may not even be visible to IT.

As the number of high-profile data breaches increases, and boards become more aware of their financial liability, cybersecurity has become a risk management exercise. CISOs are focused on managing the risks associated with shifting business goals and processes, measuring the risk associated with the devices, services, and protocols they need to implement in order to meet those goals, articulating their tolerance for risk, and then putting a plan in place to mitigate that risk. Issues that need to be considered include:

- The digital footprint of both businesses and individuals has expanded dramatically, increasing the potential attack surface.
- Everything is a target, and anything can be turned into a weapon.
- Threats are becoming intelligent, can operate autonomously, and are increasingly difficult to detect.

Part of the challenge is that this is not a greenfield problem. Your IT team has already deployed dozens of security solutions, from a variety of vendors, across your distributed network. Unfortunately, these tools were never designed to secure the highly distributed, borderless, and increasingly transient networks you are developing. These traditional security tools often operate in isolation, have separate configuration and management consoles, and require tedious hand-correlation in order to see and respond to sophisticated attacks—which is why many new threats manage to persist inside networks for months before being detected.

Buying new security hardware to load into your network to address a new network segment or threat vector is no longer a reasonable strategy. That approach runs the risk of compounding an already overly complex environment, while overwhelming the limited resources available to configure, integrate, monitor, manage, and correlate these new tools. Like your networks, security needs to be reimagined.

In this paper we will take a look at five recent networking trends, why they represent real risk to your organization, and ways to implement a new security strategy that will allow you to embrace the opportunities of the digital economy with confidence.

WHITE PAPER

1. THE INTERNET OF THINGS

Experts predict that by 2020 there will be 4.3 Internet-connected devices for every man, woman, and child on the planet. Revenue resulting from IoT is estimated to exceed $300 billion in 2020, with a global economic impact of $1.9 trillion.

There are actually three different groups of IoT devices, and likely, your organization is implementing at least two of them.

The first, Consumer IoT, includes all the connected devices we are most familiar with, such as smartphones, watches, and cars, and connected appliances and entertainment systems. Many of these devices belong to your employees, customers, and guests. They want to connect them to your network to check their mail and calendars, browse the Internet, and collaborate with others.

The other two, Commercial IoT and Industrial IoT, are made up of things most general consumers never see. Commercial IoT includes things like inventory controls, device trackers, and things like connected medical devices. Industrial IoT covers such things as connected meters and pumps, pipeline monitors, manufacturing floors, and automated industrial control systems. Implementing IoT gives you access to critical, real-time information, improves productivity and efficiency, and can provide a real competitive edge.

The security challenges of IoT are real, however, and are ones of both depth and breadth. Many IoT devices you have deployed were never designed with security in mind. They often have weak authentication and authorization protocols, easily exploitable software and firmware, poorly designed communications systems, and little to no security configurability. Many are "headless," which means that you cannot install security clients on them, or even easily patch or update them.

Infected or compromised IoT devices can spread malware and disrupt or steal critical data. As we saw last fall, vulnerable IoT devices can be weaponized and used to create massive business disruptions and denial-of-service attacks. And if your IoT devices interact with operations systems, such as manufacturing floors or critical infrastructure, the results of a compromise can be devastating.

2. MOVING TO THE CLOUD

According to Forbes, in the next few years 92% of workloads will be processed by cloud data centers, while only 8% will continue to be processed by traditional data centers. The opportunity to offload the capital and operational expenses associated with purchasing hardware infrastructure and software tools has been a key driver in the adoption of cloud computing. This is especially true when organizations look ahead and see the looming volume of data that they will need to consume and process in order to continue to compete in the digital marketplace.

Most CEOs and CIOs, however, cite security as a primary gating factor preventing their full adoption of a cloud-based computing model. Expanding your network into the cloud necessarily expands your potential attack surface. The biggest fear is that the cloud is often a black hole to their IT team. They can't see their data, where it is being stored, who is accessing it, or whether their local security protocols are being adequately enforced once data leaves their environment.

Like IoT, there are actually a variety of clouds. Public clouds exist outside your local domain and provide a number of services, from simple storage, cloud-based applications, or on-demand compute services to complete platform and infrastructure solutions, including consulting, design, integration, application development, and software services. Private clouds add virtualized devices and services to your traditional network, allowing you to better manage overhead and resources while automating many IT functions that used to require manual intervention.

While nearly all cloud providers offer a wide variety of security solutions and SLAs designed to protect your intellectual property and critical data, there are still a number of security issues that need to be considered and understood before making the leap into the cloud.

- Can I see and track my data as it moves between cloud environments?
- How do I prevent my data from being stored with unapproved cloud service providers?
- What tools are available that let me enforce consistent policies regardless of where my data resides?
- Can I see and respond to malicious traffic that originates from or has passed into my cloud environment?

The weakest link in cloud security, however, is not in its architecture. It lies in the millions of remote devices accessing cloud resources. Cloud security depends on controlling who is let into the network and how much they are trusted. We expect to see more attacks designed to exploit endpoint devices, resulting in attacks designed to target and breach cloud providers.

3. RANSOMWARE

In spite of more money and resources being spent than ever before, sophisticated attacks continue to bypass organizational defenses and grab headlines. Part of the reason is that threats are getting smarter and harder to detect. The other is human nature. Someone in your organization is going to be tricked into clicking on an infected link or attachment that injects some sort of malicious code into your network, no matter how many times they are warned.

The primary driver for most cyberattacks is financial, and nothing demonstrates this more than the dramatic rise in ransomware. According to some experts, the total cost of ransomware for 2016 topped a billion dollars, and this success is likely fueling its continued growth.

Of course, holding high-value assets hostage in exchange for some sort of payment is not new. But we have also begun to see the growth of a troubling new trend in this area. Ransomware as a service allows fledgling cybercriminals to now participate with virtually no technical training or skills. New, cloud-based "franchises" provide access to sophisticated hacking and ransom tools

in exchange for a low upfront investment coupled with back-end profit sharing. This has led many experts to predict that ransomware will continue to experience exponential growth, in part by being able to cost-effectively spread to lower-profile organizations in less traditional markets.

While organizations will continue to see broad-based attacks against high-value targets, such as data centers or communications systems, they are also likely to see an increase in targeted attacks designed to collect and hold hostage intellectual property or even sensitive or personal data.

We also expect to see the price of ransom demands to get much higher. But the impact to affected organizations goes beyond money. Public ransomware attacks can undermine consumer confidence and deflate brand value. And for some organizations, failure to have adequately prepared for such an attack may also include legal consequences.

4. SSL ENCRYPTED DATA

The volume of traffic that today's networks need to consume and process has begun to overwhelm their security devices. But the challenge for security isn't just limited to traffic volume. Because of the sensitive or proprietary nature of much of this data, traffic also needs to be secured using things like SSL encryption.

Encrypting data sounds like a good idea. Even if cybercriminals manage to breach your network, anything they manage to intercept and steal will be useless. But what's good for you can also be good for them. Encrypted traffic can also hide malware, network probes, and malicious traffic. So, it all needs to be broken open, inspected, repackaged, and sent on its way.

Which is easier said than done.

Inspecting things like SSL traffic is extremely resource-intensive. As a result, most security devices on the market today take huge performance hits when inspecting encrypted traffic—and just when performance is more critical than ever. As a result, many organizations are choosing to either not encrypt critical traffic or not inspect encrypted traffic, either of which introduces unnecessary risk into an already complicated threat landscape.

5. THE CYBERSECURITY SKILLS GAP

To add to the complexity of the problem, we are also facing a severe global shortage of skilled cybersecurity professionals. Estimates run as high as a million unfilled cybersecurity jobs globally. In a recent survey conducted by the Information Systems Security Association (ISSA) and analyst firm Enterprise Strategy Group (ESC), 70% of organizations say that the cybersecurity skills gap has had an impact on them, including 54% who claim that a security event experienced in the previous year was the result of the lack of security staff or training.

You can't plan, design, implement, manage, analyze, assess, or improve your security posture if you don't have people on your team with adequate security skills who also understand your short- and long-term business objectives and the security ramifications of the radical changes happening in the network.

SO, WHAT DO YOU DO?

To meet the demands of today's new digital business requirements, organizations need to rethink their traditional, siloed approach

to selecting and deploying security tools. Isolated security strategies increase overhead, reduce visibility, and restrict control.

Today's security challenges can only be managed by transitioning to a holistic security strategy. Sophisticated networks require high-speed authentication and monitoring, internal segmentation to automatically separate and monitor sensitive resources, the integration and automation of traditionally isolated security technologies, and cloud-based security services that can track and defend devices and data distributed anywhere across your ecosystem of networks.

An integrated security fabric ties the entire distributed network together by securely connecting endpoint and IoT devices with local networks and across the cloud for complete IT visibility. It synchronizes network and security intelligence, expands visibility, and automates control across the distributed enterprise to detect and defend against advanced threats.

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

Jan 30, 2017