FORTINET

DIGITAL TRANSFORMATION MUST INCLUDE SECURITY

WHITE PAPER

As businesses retool to compete more effectively in the new digital marketplace, new data requirements make it imperative that their networks run faster and more efficiently. Collecting data from a variety of sources, including new IoT devices with encrypted data, and then processing it to produce and deliver valuable and competitive information is the foundation of the new digital economy.

Not surprisingly, traditional network architectures—built on legacy network devices accumulated over time from dozens of different manufacturers—were never designed to support today's requirements for power, flexibility, and efficiency. While most enterprises originally deployed solutions from dozens of manufacturers to avoid a single point of failure, doing so actually degrades their security posture by minimizing threat correlation capabilities while increasing management complexity.

So, over the past few years, enterprises have been rapidly replacing their network hardware with virtualized servers and cloud-based infrastructures and reducing the numbers of vendors they work with. This consolidation process not only enables IT and data-center efficiency, but also reduces ongoing capital and operational expenses. Fewer devices, from fewer vendors, means that limited IT resources can be refocused on driving the organization's core business. Vendor consolidation also reduces the number of management consoles that need to be monitored, improves visibility and control, and enables increased automation.

As more and more edge devices move into the cloud, and the network becomes more distributed and transient, however, traditional perimeter-based security strategies also need to change. Ironically, just as networking overhead is being reduced, the number of specialized security devices showing up across the network is expanding.

There are two things driving the expansion of security devices and vendors in the enterprise.

The first is that while the number of vendors and physical devices that need to be managed are being reduced, the network itself has become more complex. Data and resources are being spread across a variety of domains, including public and private clouds, mobile endpoint devices, and remote offices, and networks themselves are no longer static. Traditional security tools have a difficult time simply keeping track of dynamic, responsive, and increasingly transient networks, let alone inspecting and securing the growing volume of data, devices, and users on those networks.

Second, the nature of cyber crime is changing as well. Attacks, like the current rise in ransomware, are becoming both more complex and costly. In addition, new multistage attacks have not only adopted self-learning and sophisticated evasion techniques, but are aimed at a variety of attack vectors across the distributed network, including the wide variety of endpoint devices and cloud environments. They also exploit the limitations inherent in many current security deployments by moving laterally across an organization to evade detection.

To address these challenges, organizations are buying and deploying specialized security tools designed to address both new threats as well as operate in new environments, supporting such things as hypervisors, cloud environments, access points, and endpoint devices. However, these solutions are quite often simply more of the same—isolated devices that require additional resources to deploy, tune, and manage.

The resulting challenges are predictable.

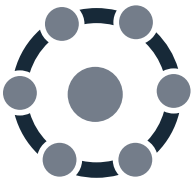
- **Increased IT overhead**—Security devices require tuning, updating, and managing, and as network environments automatically change to meet shifting workload, data volume, and traffic requirements, security rules need to be updated and changed to secure these evolving network paradigms. The fact is, this can no longer be done by hand. Each new tool requires an engineer who is familiar with its configurations and OS, can tune it to the network segment it is assigned to protect, and can keep its security data and threat intelligence updated. That often adds up to more staff than most organizations can afford. So security tools often run at suboptimal efficiency, some data and network segments are often left poorly secured, and erratic and unpredictable update cycles leave devices vulnerable or less effective.
- **Complex management**—Each security solution family usually has its own management console that only provides insight into the tools and data it is designed to control. Multiply this by a dozen or more security vendors, and you have a logistical management nightmare. Even more challenging, these devices were never designed to share threat intelligence, so IT teams are forced to hand correlate information in order to discover today's more sophisticated threats. This means the time between your networking being compromised and the threat being discovered is often measured in weeks, rather than the minutes or seconds you really need to effectively defend your assets.
- **Isolated devices can't react as a system**—Once a threat has been discovered, you need to know where it came from, how long it has been there, which devices have been compromised, and how to clean it up. This means your security solutions need to be able to synchronize a coordinated response to any detected threat. Unfortunately, isolated devices can't do that; therefore, some segments of your network may get overlooked. Far too often, private or public cloud environments remain a blind spot as far as security is concerned.
- **Security skills gap**—Even worse, all of this is happening at a time when seasoned professionals with the security training and skills you need are increasingly scarce. Experts estimate that there are currently one million unfilled cyber security jobs worldwide, with that number increasing to 1.5 million by 2019.

LAYERING AUTOMATED SECURITY

Like the networks they need to protect, security needs to be rethought and retooled. To support today's dynamic networks, security needs to see every device on the network, establish policy at the point of access, and monitor and protect data and resources as they move across the distributed environment, from IoT, across the network, and into the cloud. This requires an architectural or fabric-based approach to security that enables cross-integration, seamless collaboration, and automated adaptability.

To achieve this, you need to begin replacing your legacy and isolated security devices and platforms with tools designed to work together using either a common OS or built around common standards. Where possible, move to a single vendor that enables unified management and control for solutions deployed in physical, virtual, cloud, and remote locations for consistent policy orchestration and enforcement. When that's not possible, look for solutions that support open standards so they can be seamlessly integrated into your security and management framework.

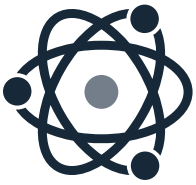
Tools that can be woven together into a holistic security fabric will always provide better visibility and control than those that only operate in isolation. They can actively collect and share threat information to improve visibility and intelligence, enhance situational awareness, and enable a synchronized attack response anywhere in the network. Such an approach allows organizations to address three fundamental security requirements demanded by today's networks:



BROAD

Any effective security deployment needs to cover the entire attack surface and respond in real time to both detected threats and dynamic changes to the network. Network administrators need to have visibility across the entire environment, including endpoints, access points, IoT devices, network elements, the data center, the cloud, and even the applications and the data itself, through a single pane of glass.

A unified view across the extended and increasingly elastic enterprise cannot be built around isolated devices. A security framework based on open standards enables solutions to operate as a unified system. Such an approach helps administrators tie together data, applications, devices, and workflows to find and respond to today's most sophisticated threats anywhere across the distributed enterprise.



INTEGRATED

Many of today's most advanced threats are designed to evade detection. They bypass edge security gateways by hiding in encrypted traffic, using multistage attacks that initially appear harmless, tricking users into downloading and running a malicious executable, or by being introduced directly into the network through an infected mobile device. Once inside, they spread laterally across the network by observing and mimicking legitimate traffic patterns. They may also lie dormant for long periods of time, waiting for a command or circumstances to activate them. As a result, a successful infiltration may remain undetected inside a compromised network for weeks or months, gathering and exfiltrating sensitive data.

One of the factors contributing to this challenge is that many of the security tools that organizations have distributed across their network run in isolation. They only see the traffic that passes in front of them, and can't share or correlate threat intelligence to see the bigger picture that is required to detect these advanced threats.

This problem is especially compounded when data and workloads move between things like traditional and multi-cloud domains. Far too often, security specialists are forced to review logs on separate consoles and then hand correlate data to detect advanced threats. But with an average of over 30 different point products running inside a typical enterprise network, the scale of the challenge is beyond the resources most IT teams have available.

What organizations need are security devices designed to see, share, correlate, and respond to threats. This means that security tools need to be selected not only for their performance and features, but also for their ability to function as part of an integrated security system. This means they need to use a common operating system or be built around open standards. They also need to be able to operate through a centralized analysis and management system that can correlate data and orchestrate an automated response to a detected threat. Security designed around a framework of integrated devices allows complex threat behaviors and patterns to be more easily identified, compromised devices or network segments to be dynamically isolated and remediated, malicious malware to be traced back along the attack chain to its origin, and distributed security tools to operate as a system to provide continuous trust assessment across the entire distributed network environment.

AUTOMATED

Because an attack can compromise a network in minutes, visibility alone isn't enough. An integrated security architecture that ties security solutions together into a holistic solution enables fast and coordinated responses to threats. It not only allows security elements to rapidly exchange both local and global threat intelligence but also automatically synchronizes a coordinated response to isolate and remediate infected devices, update policies, search for similar outbreaks, automatically harden network segments and access points, elevate indicators of compromise, and remove malware.

In today's elastic network environments, security solutions need to automatically adapt to changing network configurations by establishing and enforcing new policies as the environment being protected adapts to shifting business needs. At the same time, additional security measures and countermeasures need to be updated or provisioned automatically as new devices, workloads, and services are deployed. This also needs to include automated auditing and security adjustments to consistent compliance even as networks are changing.

BENEFITS OF A SECURITY FABRIC

The benefits to consolidating security are similar to those derived from consolidating your network resources: reduced costs for both capital and operating expenses, increased visibility and control, reducing the scope of your security deployment, faster disaster recovery, and simplified and scalable compliance with regulatory requirements.

The Fortinet Security Fabric is the first framework to provide a complete architectural approach to security. It allows you to connect distributed security solutions into a unified framework so they can dynamically adapt to your evolving IT Infrastructure and defend its rapidly changing and increasingly distributed attack surface. In addition, its open standards design allows you to integrate software and solutions from a variety of vendors to enable seamless protection and actionable threat intelligence across all points in your network, from IoT to the cloud.

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

90833 0 0 EN February 7, 2018 1:32 PM

Mac:Users:susiehwang:Desktop:Susie Projects:2017:WP-ENT-FW-IT-Transformation:wp-ent-fw-digital-transformation-020718-131pm