HOW FORTINET SECURITY FABRIC ADDRESSES ENTERPRISE SECURITY CONCERNS

CONTENTS

INTRODUCTION

Digital transformation (DX) refers to the integration of digital technology into all areas of your business. This, in turn, results in some fundamental changes to how your business operates and how you deliver value to customers.

One key area of impact is security. The DX revolution is simultaneously increasing business vulnerability because of a few key factors:

- **Today's digital attack surface is larger than ever before, and it is constantly expanding.**
- **The complexity of managing security is difficult and becoming more challenging.**
- **Advanced threats continue to evolve and are harder to combat.**

As a lock-step extension of these changes, network security must transform as well. Protecting dynamic, distributed environments under these conditions requires broadly integrated security technologies that share intelligence, work together to detect threats, and synchronize automated responses in real time.

01 CHALLENGES: UNDERSTANDING THREAT TRENDS FOR ENTERPRISE

To protect enterprises, let's take a look at what's happening within the threat landscape and how it will evolve into the foreseeable future. There are several trending areas of interest when it comes to defining and designing an enterprise-class network security strategy.

The Expanding Digital Attack Surface. The proliferation of **cloud technologies** has certainly exposed businesses to new threat vectors. While most cloud providers offer some sort of shared responsibility for protection, organizations are still required to establish controls for hosted applications and data. The primary challenge for security becomes establishing and maintaining consistent policy and enforcement as applications migrate between local data centers and third-party cloud environments. This becomes critical as more and more enterprise data is hosted in consolidated and often multi-tenant clouds, especially with big data collected from Internet of Things (IoT) devices.

The **Internet of Things** has also introduced new risks to networks. Many IoT products 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. An IoT system breach can spread malware, steal critical data, and disrupt operations. In the context of medical services, heavy industrial systems, or public utilities, the results of a compromise carry disastrous potential.

With so many devices and cloud services, as well as industry regulations around data privacy, **Secure Sockets Layer (SSL) encryption now** accounts for nearly 60 percent of network traffic today, and it continues to grow annually.[1] And SSL inspection for security purposes can be challenging due to network performance degradation, certificate management issues, among other factors. As a result, many organizations are opting not to encrypt and/or inspect critical traffic, websites, cloud applications, and email.[2] But this poses a problem, as cyber criminals can also use SSL encryption to conceal malware and ransomware from traditional enterprise security solutions, thus making inspection a critical requirement. The challenge is that SSL decryption and traffic inspection over traditional network security solutions causes network latency and performance degradation that disrupts business operations.

Increased Complexity of Managing Security. As a result of this expansion and an increasingly invisible network boundary, many organizations have turned to using an assortment of **different point products** to secure the various extensions and exposures of

their distributed businesses. This kind of security typically lacks network-wide automation and intelligent communication between the disparate parts—which can lead to lapses in protection.

[1] "Q4 2017 Threat Landscape Report," Fortinet, February 2018.
[2] "The Rapid Growth of SSL Encryption: The Dark Side of SSL That Today's Enterprise Can't Ignore," Fortinet, April 2017.

Advanced Threat Proliferation. Overall, FortiGuard Labs saw more than 17,000 unique malware variants in 4Q17, and ransomware attacks more than doubled last year.[3] A robust cyber crime ecosystem enables fast creation of new malware versions of successful attacks. Further, businesses are likely to continue seeing an increase in targeted attacks against high-value targets (e.g., data centers and communications systems) to collect and hold hostage intellectual property and sensitive data. The impact includes not only the money paid but also the public exposure associated with these sorts of incidents, which can undermine consumer confidence and deflate brand value. For some organizations, the failure to adequately prevent such an attack may even include legal consequences.

At the same time that advanced threats are increasing, we are also facing a severe global shortage of skilled cybersecurity professionals. Estimates run as high as one million unfilled cybersecurity jobs worldwide. More than 50 percent of IT leaders indicate that a shortage of cybersecurity staff has increased the workload on existing staff, and 35 percent have compromised on filling roles with the right skills and experience. Over half disclosed that their organizations have experienced at least one cybersecurity event tied to their lack of security training and staff resources.[4]

[3] Tara Seals, "Cyberattacks Doubled in 2017," Infosecurity Magazine, January 26, 2018.
[4] Jon Oltsik, "Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II)," ESG and ISSA, December 2016.

02 THE FABRIC APPROACH TO SECURITY

An open, end-to-end **security fabric** approach is an architectural approach that protects the entire attack surface and provides a comprehensive view of all the security elements, which allows organizations to address the full spectrum of challenges they currently face across the attack life cycle. Integration and interoperability should not only be requirements for all parts of the fabric but also part of any foundational security policy or strategy.

This security fabric would be able to consistently distribute, orchestrate, and enforce policies across different domains—including remote workers, branch/retail offices, geographically distributed data centers, and private/public cloud networks. It should:

- **Broadly cover all parts of the organization** as it grows and changes
- **Integrate security components into a unified solution** to better detect advanced threats
- **Take automated, intelligent action** as a single, cohesive system

A security fabric approach reaches both deep and wide across the entire distributed network. It works as a unified system that shares between components. Its broad interoperability between all the various solutions that protect these distributed domains provides critical visibility under rapidly changeable network conditions.

As a result of this broad awareness, the fabric can then make fast and coordinated responses to threats—allowing all elements to rapidly exchange threat intelligence and coordinate actions. It launches synchronized defenses against attacks based on real-time global and local threat intelligence, isolating affected devices, removing malware, partitioning network segments, updating rules, and pushing out new policies.

03 THE FORTINET SECURITY FABRIC

The Fortinet Security Fabric connects critical security and networking technologies—from firewalls to content and application security to secure access points—for seamless security across the distributed network, whether local or remote, physical or virtual, wired or wireless, and in your domain or in the cloud. It was built on three key attributes:

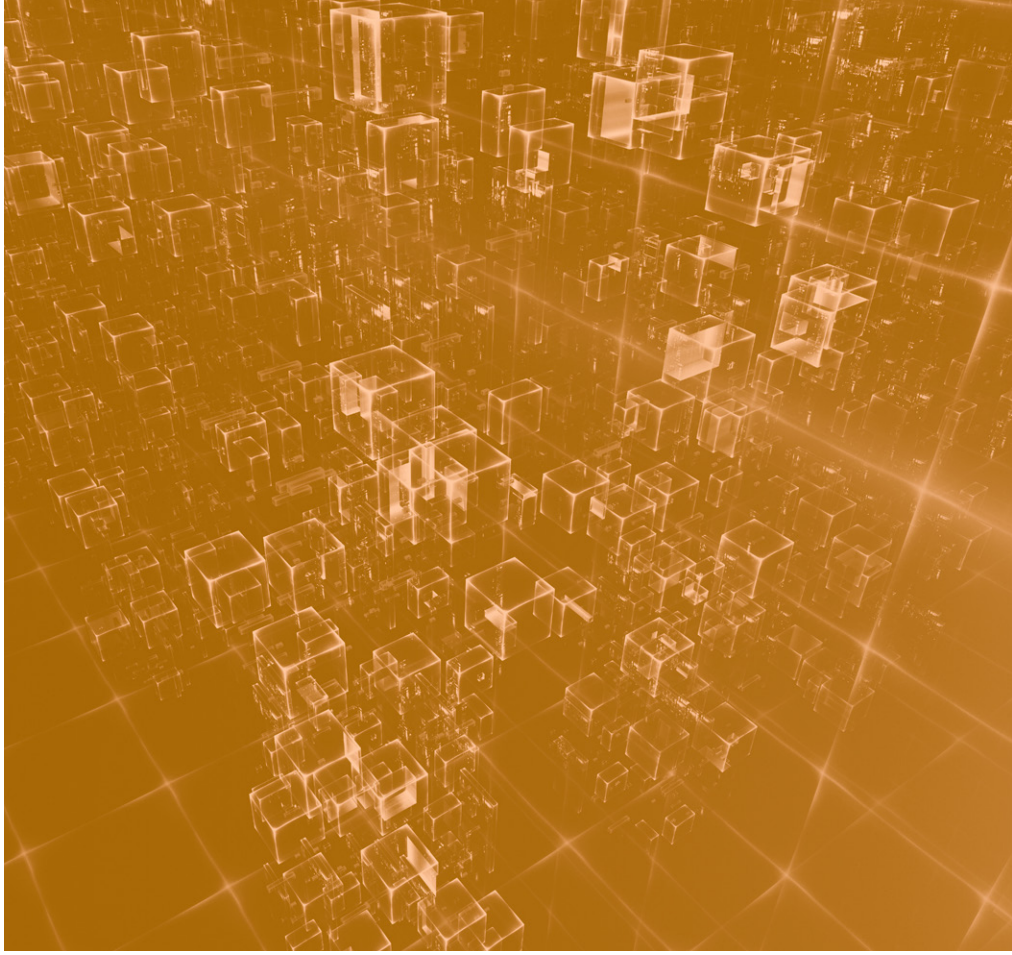
BROAD: Our Security Fabric covers the entire attack surface. Administrators enjoy visibility and protection across the complete infrastructure, including endpoints and IoT devices, access points, network elements, the data center, the cloud, and even the applications and the data itself.

Fortinet Security Fabric seamlessly enables strong security from endpoint devices to the access layer for wired and wireless networks. It scales from the smallest branch deployments to the largest, most complex, and data-intensive campus and data center environments, plus virtual protection for private, hybrid, and public clouds.

INTEGRATED: An expanded network attack surface combined with ever-increasing threat sophistication presents a high degree of risk for today's enterprises, even with the traditional protections in place. Organizations need all the different parts of their security infrastructure to work as a single, well-oiled machine. Our Security Fabric is designed not only for integrated protection across all the devices and systems protecting the distributed network, but also rapid detection of advanced threats as well.

AUTOMATED: Because an attack can compromise a network in minutes, visibility isn't enough. Our Security Fabric takes fast and coordinated action against threats, allowing the right elements within the infrastructure to rapidly exchange threat intelligence and synchronize responses. Our approach allows the network to automatically see and dynamically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware.

Fortinet Security Fabric also empowers solutions to dynamically adapt to changing network configurations and establish and enforce new policies as business needs shift within the environment. Security measures and countermeasures are provisioned automatically as new devices, workloads, and services are deployed across the infrastructure. The Security Fabric also supports open application programming interfaces (APIs), which allow organizations to integrate existing security and networking investments into the Fortinet Security Fabric.



04 HOW FORTINET SOLUTIONS ADDRESS TODAY'S THREAT TRENDS

By design, the different parts of our Security Fabric work collectively to address the aforementioned threat trends that enterprises face.

Network Security: Our fabric-enabled network security encompasses products and services that provide high-performance protection and deep visibility across the breadth of the infrastructure. It offers the ability to call upon threat protection anywhere in the network to counter both known and unknown attacks.

The Fortinet Security Fabric's auditing functions support best practices for ensuring risk reduction and improving the network's security posture. It also orchestrates segmentation from the branch, to the core, to the data center, to the cloud. So, if a piece of encrypted malware makes it inside the network perimeter, it won't go far before being detected and contained.

Multi-Cloud Security: The Fortinet Security Fabric was designed to extend deep into different cloud environments to ensure consistent policies and enforcement across the distributed resources with access. Within the unified security architecture, virtual firewalls can be deployed across private, public, and hybrid clouds to establish north-south and east-west microsegmentation.

Our Security Fabric weaves cloud applications into the broader environment—governed by seamless, universal security and compliance policies and managed via transparent visibility across the entire attack surface. Combining Fortinet Cloud Security with an existing enterprise firewall deployment extends the same powerful security at scale, as well as the same intelligence and dynamic risk mitigation to applications located either in the cloud or on-premises.

Endpoint Security: Network defenses must detect and block malicious objects delivered via web, email, network, or personal storage to an endpoint. Our fabric-enabled endpoint security integrates single-pane-of-glass visibility and control and automates endpoint protection of known and unknown threats (exploits and malware) via cloud-based global intelligence and sandboxing.

Secure Unified Access: Our Security Fabric goes well beyond just integrating security solutions. Fortinet's Secure Access solution extends common security policies to the very edge of the wired and wireless network—where highly vulnerable IoT devices reside and where potentially compromised, trusted laptops and phones connect. 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 IoT devices into a centralized management view and then applying access control and response. The Fortinet Security Fabric can do that, as well as protect the network against known and trusted laptops or phones that become infected while off the network. The integration of the Fortinet Security Fabric elements enables policy enforcement that is pushed to the point of access for the protection of all network assets.

Email Security: Another critical need is inspecting email for unwanted (spam) and malicious (phishing, malware) messages, as well as inappropriate or sensitive content. Fortinet email security delivers protection from established attack classes with a powerful mix of traditional prevention technologies. Further, because it is Fortinet Security Fabric-enabled, it combats advanced email threats by leveraging integrated sandboxing. This provides automated responses through indicators of compromise (IoC) sharing. Enterprises also gain consolidated visibility of their enterprise-wide security posture via logs sent to a central analytics platform.

Web Application Security: The influx of web-based applications into the enterprise rapidly increases the need for comprehensive web application security. Our fabric-enabled web application security offers advanced persistent threat protection with file scanning of application attachments. It helps protect distributed operation through shared threat intelligence across network segments. These features also integrate with other third-party services for even more extensive vulnerability protection.

Advanced Threat Protection (ATP): Combating the steady stream of malware, including ransomware, requires new, advanced detection techniques such as sandboxing to keep pace with the rapidly changing (and often highly targeted) campaigns. Further, it must be infused within a security fabric that covers the different delivery channels cyber criminals employ to gain entry—email links and attachments, website downloads, web-based infrastructure, end-user computing and even compromised IoT devices.

As part of the Fortinet Security Fabric, the Fortinet ATP solution can inspect traffic at any or all entry points. Dynamic intelligence sharing coordinates response and improved defense across the digital attack surface. APIs enable the sharing of this intelligence among both Fortinet and non-Fortinet components for seamless defense across security elements throughout the organization.

Management and Analytics: The Fortinet Security Fabric delivers seamless management and analytics tools to help uncover hidden insights while reducing the total cost of ownership (TCO) for your security infrastructure.

These functions enable shorter deployment times and fewer misconfigurations due to simplified security configuration across the attack surface. They also help discern the highest priorities via a single point of inspection that considers telemetry from across the entire attack surface. These features also increase security effectiveness through capabilities such as next-level analysis, which automatically validates security operations insights against accurate network operations-built attack surface views.

CONCLUSION

While undergoing digital transformation, enterprises face unprecedented changes in terms of network evolution and an aggressively adaptive threat landscape. But a security fabric approach offers IT leaders a coordinated, multi-defense response from across today's distributed infrastructures—from end to end.

The Fortinet Security Fabric presents an architectural approach that connects multiple solutions to form a unified security framework. It helps enterprises dynamically adapt to their evolving IT infrastructures to defend a rapidly evolving attack surface and landscape.

FORTINET®

www.fortinet.com

175547-A-0-EN