




A CISO GUIDE TO MODERN SECURITY ARCHITECTURE:

**Implementing a Fabric Architecture to Secure the
Entire Organization, Meet the Demands of Compliance
and Governance, and Proactively Manage Risk**



CONTENTS

INTRODUCTION	1
SECTION 1: UNDERSTANDING SECURITY CHALLENGES FOR ENTERPRISE	2
SECTION 2: THE FABRIC APPROACH TO SECURITY	4
SECTION 3: THE FORTINET SECURITY FABRIC	6
SECTION 4: HOW FORTINET SOLUTIONS ADDRESS TODAY'S THREAT TRENDS	8
CONCLUSION	11





INTRODUCTION

It's common for companies to expand their digital networks to keep pace with expanding business demands. As a natural extension of this growth, network security needs to increase at the same time. But today's security climate is very different than it was even just a few years ago, compounding risk.

Several changing factors make this topic a serious consideration when it comes to the strategic expansion of an enterprise:

- The associated risks and performance burden of **SSL-encrypted data**
- **Cloud** enforcement

- **Internet of Things** (IoT) vulnerabilities
- The rise of **ransomware**
- The current **shortage of skilled IT security staff**

Securing dynamic, distributed environments under these challenging conditions requires tightly integrated security technologies that share intelligence, work together to detect threats, and synchronize automated responses in real time.



01 UNDERSTANDING SECURITY CHALLENGES FOR ENTERPRISE

To protect enterprises, we need to first understand what's happening within the threat landscape today and into the foreseeable future. There are several trending areas of interest when it comes to defining and designing an enterprise-class network security strategy.

SSL-Encrypted Data: Many organizations must encrypt certain types of sensitive data in transit using Secure Sockets Layer (SSL) to comply with industry regulations. SSL traffic accounts for 35 percent to 50 percent of network traffic today,¹ and it continues to

grow annually.² But cybercriminals can also use SSL encryption to conceal malware and ransomware from traditional enterprise security solutions. SSL decryption and traffic inspection with traditional network security can experience network latency and performance degradation that disrupts business operations. As a result, many organizations are choosing to either not encrypt critical traffic or not inspect encrypted traffic.

Cloud: Even though most cloud providers do offer some sort of protection, their security measures are almost certainly outside the control of your

organization. The primary challenge for security becomes establishing and maintaining consistent policy and enforcement as data moves back and forth between local networks and third-party cloud environments. As more and more enterprise data is being stored in consolidated and often multi-tenant clouds, especially with big data collected from IoT devices, a key area of focus should be ensuring that endpoint, IoT, and other edge devices don't become a conduit for malware injection into the cloud.

IoT: 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.

Ransomware: Ransomware attacks more than doubled last year. 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.

Skills Shortage: We are currently facing a severe global shortage of skilled cybersecurity professionals. Estimates run as high as a 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.³

02 THE FABRIC APPROACH TO SECURITY

An open, end-to-end security **fabric** (which can scale and adapt to changing network demands) 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** detection and response to 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:

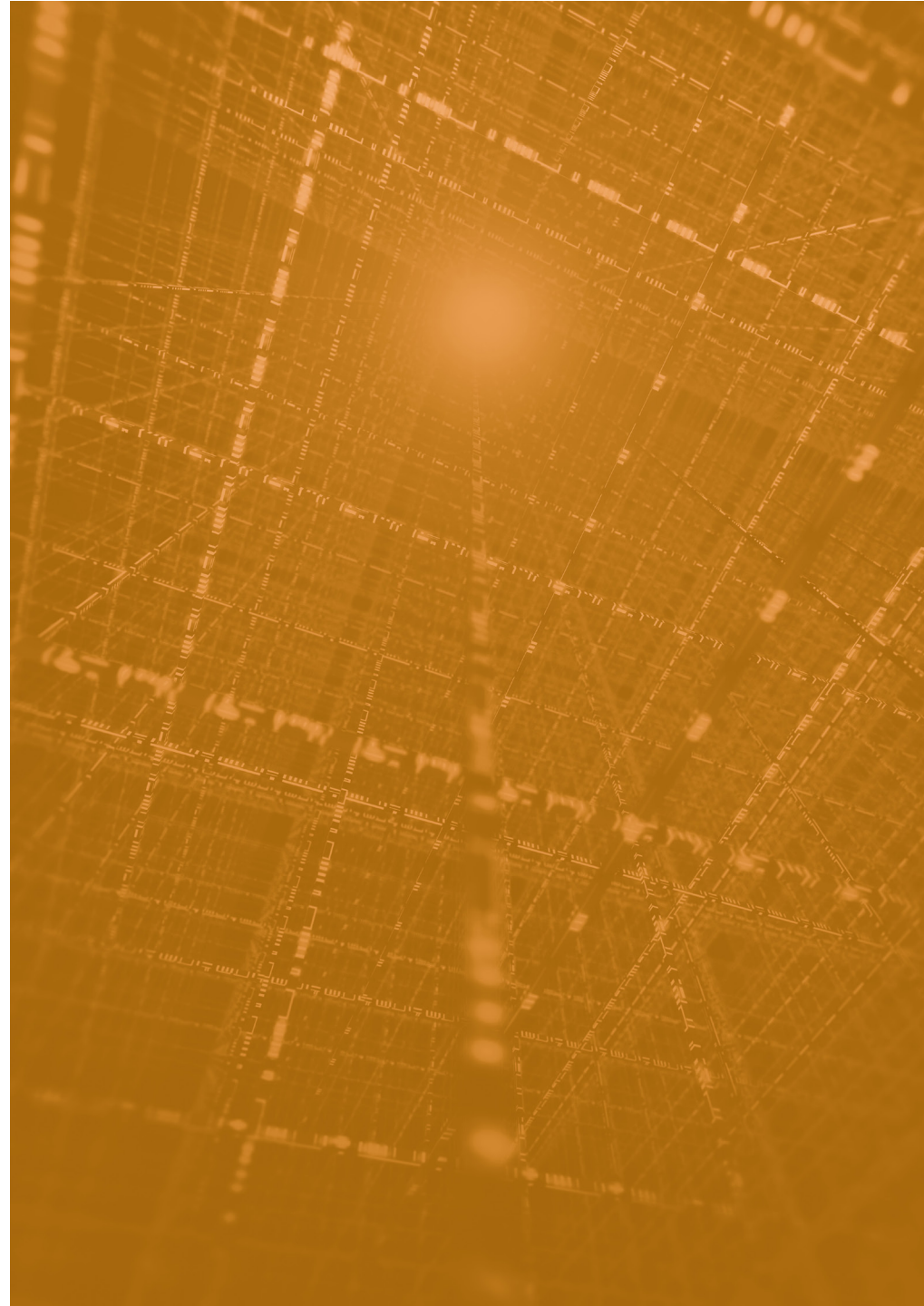
BROAD: Our Security Fabric covers the entire attack surface. Administrators enjoy visibility across the complete infrastructure, including endpoints, IoT devices, access points, network elements, the data center, the cloud, and even the applications and the data itself.

This allows security to cover all potential entry points as well as segments inside the dynamic network. Such broad deployment and deep visibility aids in compliance, helps monitor internal traffic and devices, prevents unauthorized access to restricted data and resources, and controls the spread of intruders and malware.

INTEGRATED: Enterprises average more than 30 point security products within their environments, resulting in multiple time-consuming security consoles and lack of transparency. The Fortinet Security Fabric streamlines communications among the different security solutions, shrinking detection and remediation windows.

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.

The 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 today's enterprises face.

Enterprise Firewalls: Our Security Fabric enables high-performance SSL decryption and inspection processes for both inbound and outbound communications across the entirety of the attack spectrum. The Security Fabric is built on the core of Fortinet's Enterprise Firewalls—for branch, campus, data center, and internal segmentation deployment—all interconnected by a single, unified operating system for simplified and coordinated deployment and control.

These capabilities provide the industry's highest-performing, most secure defense against known threats and support industry-mandated ciphers.

Our Enterprise Firewall solution allows segmentation of network elements, enforcing traffic, device, and data separation for stronger control. So, if a piece of SSL-encrypted malware makes it inside the network perimeter, it won't go far before being detected and contained. It also performs SSL inspection—decrypting traffic to apply threat prevention controls.

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.

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.

Secure Access: The Security Fabric goes well beyond just integrating security solutions. Fortinet's Secure Access solution extends coordinated security policies to the very edge of the wired and wireless network—where highly vulnerable IoT devices reside.

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. But the Fortinet Security Fabric can integrate all 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 the different attack surfaces.

Advanced Threat Protection (ATP): Combating ransomware attacks requires a security fabric that covers the different delivery channels cybercriminals employ to gain entry—email links and attachments, website downloads, business application delivery, social media sharing, and even compromised IoT devices. As part of the Security Fabric, Fortinet's Advanced Threat Protection solution can be deployed at any or all entry points with rapid global intelligence to impede the volume of ransomware and dynamic local intelligence generated to thwart the very latest campaigns. Further, APIs enable the sharing of this intelligence among Fortinet and non-Fortinet components for that seamless defense across security elements throughout the organization.

Our ATP components work together to automatically and continuously hand off objects and data from one to the next to prevent, detect, and mitigate attacks across the entire environment and all attack vectors.

They also can monitor outbound communications for ransomware-encrypted command and control communications, as well as sophisticated malware replete with evasion techniques.

Security Operations: Adaptive visibility and control across the Fortinet Security Fabric is a requirement for the security operations team tasked with monitoring and responding to incidents throughout the organization. The Security Fabric's Security Operations tools help to manage, monitor, and report on multiple fabric components from a single control point—whether they include multiple instances of the same Fortinet product, multiple Fortinet products, or multiple products from multiple vendors. Prebuilt reports help with managing compliance across the enterprise infrastructure.

With the number and virulence of threats growing and the complexity of security architectures increasing, our fabric approach to security operations offers a compelling alternative to point and platform solutions that require cybersecurity staff who are trained and well-versed on multiple product and solution

components. It alleviates the urgent need to hire additional IT security specialists, while enabling existing cybersecurity staff to scale in their support in a simplified, unified manner. The ability to self-discover network-attached elements creates a dynamic centralized management database (CMDB).





CONCLUSION

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

The Fortinet Security Fabric presents a compelling approach that connects multiple solutions to form a unified security framework. It helps today's enterprises dynamically adapt to their evolving IT infrastructures to defend a rapidly evolving attack surface.

1. 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," SecurityWeek, March 15, 2016.
2. Butler, "SANS Institute InfoSec."
3. Jon Oltsik, "[Through the Eyes of Cyber Security Professionals: Annual Research Report \(Part II\)](#)," ESG and ISSA, December 2016.

The Fortinet logo is displayed in white, bold, sans-serif capital letters. The letter 'F' is stylized with a series of horizontal bars of varying lengths, creating a digital or network-like appearance. A registered trademark symbol (®) is located to the right of the word.

FORTINET®

www.fortinet.com

Copyright © 2018 Fortinet, Inc. All rights reserved. 223091-A-0 06.13.2018