FORTINET

4 Critical Considerations for Security Architecture Design

Introducing Fortinet Security Fabric for Broad, Integrated, Automated Security

Table of Contents

Executive Overview

Organizations are rapidly adopting digital innovation (DI) initiatives to accelerate their businesses, reduce costs, improve efficiency, and provide better customer experiences. To accomplish DI outcomes while minimizing complexity and effectively managing risks, organizations need to adopt a cybersecurity platform that provides visibility across their environment and the means to easily manage both security and network operations.

The Fortinet Security Fabric solves these challenges with broad, integrated, and automated solutions that enable security-driven networking, zero-trust network access, dynamic cloud security, and artificial intelligence (AI)-driven security operations. Fortinet offerings are enhanced with an ecosystem of seamless integrated third-party products that minimize the gaps in enterprise security architectures, while maximizing security return on investment (ROI).

84% of security executives believe the risk of cyberattacks will increase.[1]

Digital Innovation Is Transforming All Industries

Across economic sectors worldwide, DI is seen as an imperative to business growth and improved customer experience.[2]

From the perspective of cloud service provider IT and cybersecurity leaders, DI translates into a variety of changes to their network environments. Users are increasingly mobile, and they are accessing the network from locations and endpoints that are not always under corporate IT control. They are also connecting directly to public clouds to use key business applications, such as Office 365. Outnumbering the human-controlled endpoints are Internet-of-Things (IoT) devices, which are widely distributed, often in remote and unsupervised locations. Finally, cloud service provider business footprints are diffusing into numerous and far-flung branches, most of which connect directly to cloud and cellular services, bypassing corporate data centers.

All these changes render obsolete the concept of a defensible network perimeter, requiring cloud service providers to adopt a new multilayer defense-in-depth strategy.

77% of security professionals state that their organization has moved applications or infrastructure to the cloud despite known security concerns.[3]

Migration of Applications and Workloads to the Cloud

Almost every business has started to move some workloads and applications to the cloud—or at least plans to do so. These decisions are often driven by the desire to reduce costs and to improve operational efficiency and scalability by taking advantage of the flexibility that the cloud provides.

Cloud service providers offer a wide range of possible deployment models, from Software-as-a-Service (SaaS) to Platform-as-a-Service (PaaS).

Wary of cloud service provider lock-in and aiming to deploy each application and workload in the cloud for which it is best suited, many organizations have adopted a multi-cloud infrastructure. The downside of such freedom of choice is the need to learn the idiosyncrasies of each cloud environment. In addition, organizations must use different tools to manage the environment and its security provisions, which challenges visibility and necessitates the use of multiple management consoles for policy management, reporting, and more.

Cloud environments are dynamic: 74% of companies have moved an application to the cloud and then brought it back on-premises.[4]

Profusion of Endpoints Across Multiple Environments

Endpoints are arguably the most vulnerable nodes in the cloud service provider's network. The larger providers have thousands of employees, each using multiple work and personal devices to access network resources. Ensuring good cyber hygiene and up-to-date endpoint security on all these devices is a formidable task. Even more daunting is the proliferation of IoT devices. By the end of 2019, the number of active devices exceeded 26.66 billion, and during 2020, experts estimate that this number will reach 31 billion.[5]

IoT devices are present in numerous business contexts. They provide personalized experiences to retail and hospitality customers, track inventory in manufacturing and logistics, and monitor devices on factory floors or in power plants.

Often ruggedized and power-efficient, IoT devices focus on performance, often at the expense of security features and secure communication protocols. And unlike most network-attached devices, IoT equipment is commonly deployed in remote locations, out of doors, or in unstaffed or infrequently staffed facilities (such as power stations). From these insecure locations, the equipment frequently transmits critical, sensitive data to on-premises data centers and to cloud services.

84% of enterprises have a multi-cloud strategy. 81% point to security as a major cloud challenge.[6]

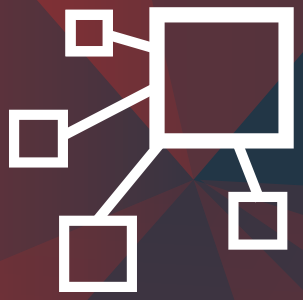
Expanded Business Presence Across Distributed Markets and Geographies

As companies expand their global footprint by opening new facilities, branch offices, and other satellite locations, they experience increasing wide-area network (WAN) bandwidth constraints. Although SaaS applications, video, and Voice over IP (VoIP) boost productivity and enable new services, they also contribute to an exponential growth in WAN traffic volume.

Highly reliable multiprotocol label switching (MPLS) has been the WAN connectivity technology of choice for many years. However, with MPLS it is difficult to optimize WAN bandwidth use and to vary quality-of-service levels as needed for different applications. As a result, branch expansion and service enhancements can quickly lead to exploding WAN costs.

Consequently, organizations are turning to software-defined WAN (SD-WAN), which makes efficient use of MPLS, internet connections, and even telecommunications links. Plus, SD-WAN dynamically routes each kind of traffic over the optimal link. Embrace of SD-WAN has further created the need for secure SD-WAN, which is best delivered as a combination of network and security functions in an integrated platform.

From 2017 to 2019, there was a 73% increase in the number of organizations experiencing data breaches due to unsecured IoT devices or applications.[7]



SD-WAN provides better performance and security at a lower cost than MPLS.[8]

Four Considerations for Security Architecture Design

As organizations proceed enthusiastically with DI initiatives, the implications for network security are often overlooked or minimized. In fact, almost 80% of organizations are adding new digital innovations faster than they can secure them against cyber threats.[9]

IT leaders should prioritize four considerations above all when designing secure architectures for their digitally innovating businesses:

1. Understand the expanding attack surface

Sensitive data can potentially reside anywhere—and it can travel over numerous connections outside enterprise control. Applications in the cloud are exposed to the internet so that every new cloud instance adds to the enterprise attack surface. IoT devices extend the attack surface to remote, unstaffed locations. In these dark parts of the attack surface, intrusions can fester unnoticed for weeks and months, wreaking havoc on the rest of the enterprise. Mobile devices and user-owned endpoints bring unpredictability to the attack surface, as users roam between corporate locations, through public spaces, and across international borders. In fact, extensive cloud migration, extensive use of mobile platforms, and extensive use of IoT devices are factors amplifying the per-record cost of a data breach by hundreds of thousands of dollars.[10]

61% of CISOs state that they have significant cloud, IoT, and mobile operations already in place.[11]

Up to 40% of new malware detected on any given day is zero day or previously unknown.[12]

This expanded, dynamic attack surface dissolves the once well-defined network perimeter and the security protections associated with it. It is much easier for attackers to infiltrate the network, and once inside, they often find few obstacles to moving freely and undetected to their targets. Therefore, security in DI enterprises must be multilayered—with controls on every network segment—based on the assumption that the perimeter will be breached sooner or later. And access to network resources must be based on least privilege and continuously verified trust.

DI initiatives mean that enterprise security teams must deploy protections for 17 different types of endpoints.[13]

2. Address how cyber threats are evolving

The cyber-threat landscape is rapidly growing as bad actors attempt to circumvent and defeat traditional cybersecurity defenses. Up to 40% of new malware detected on any given day is zero day or previously unknown.[14] Whether this is driven by increased use of polymorphic malware or the availability of malware toolkits, the growth of zero-day malware makes traditional, signature-based malware detection algorithms less effective. In addition, bad actors continue to utilize social engineering by exploiting static trust methods used in traditional security approaches. Studies reveal that 85% of organizations experienced phishing or social engineering attacks this past year.[15]

As cyber threats become more sophisticated, data incidents and breaches are more difficult to detect and remediate. Between 2018 and 2019, the time to identify and contain a data breach grew from 266 to 279 days.[16] Beyond the ability to detect and prevent an attempted attack, organizations must also be capable of rapidly identifying and remediating a successful attack. Over 88% of organizations have reported experiencing at least one incident in the preceding 12 months, demonstrating that all organizations are at risk of an attack and that cyber resiliency is critical.[17]

One-third of enterprises suffered a breach of business-critical data in the last year, which could lead to regulatory penalties.[18]

3. Simplify an increasingly complex IT ecosystem using automation

According to almost half of CIOs, increased complexity is the biggest challenge of an expanding attack surface.[19] This increased complexity is due to the fact that many organizations rely upon an array of nonintegrated point products for security. The average enterprise uses upwards of 75 distinct security solutions.[20]

This lack of security integration means that these organizations are unable to take advantage of automation in their security deployment. In fact, 30% of CIOs point to the number of manual processes as a top security issue in their organization.[21] Without security automation, CIOs require more skilled cybersecurity professionals to monitor and secure their network.

However, many organizations are unable to acquire the cybersecurity talent that they require. Estimates indicate that over 4 million cybersecurity positions are currently left unfilled, and the number is steadily growing.[22] This lack of access to necessary talent is putting organizations at risk, with 67% of CIOs saying that the cybersecurity skills shortage inhibits their ability to keep up with the pace of change.[23]

Attackers understand these challenges well, and use it to their advantage.

4. Stay ahead of increasing regulatory demands

The European Union's (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are two of the most well-known data protection regulations. However, they are far from the only ones. Every U.S. state currently has a data breach notification law, and many of them are enacting additional consumer privacy protections. Driven by political and social pressure, regulations are expected to expand in coming years, and penalties for noncompliance are becoming larger, more punitive, and more common.

Organizations must also comply with industry standards, and many struggle to do so. For example, fewer than 37% of organizations pass their interim Payment Card Industry Data Security Standard (PCI DSS) compliance audit.[24] As PCI DSS is superseded by the PCI Software Security Framework (PCI SSF), these organizations are likely to face even greater obstacles to remain compliant.

The need to achieve and maintain regulatory compliance has significant impacts on an organization's ability to achieve security transformation objectives—and also informs how organizations invest in technology solutions. For example, of the 71% of organizations that have moved cloud-based applications back to on-premises data centers, 21% did so to maintain regulatory compliance.[25]

The Fortinet Security Fabric

The Fortinet Security Fabric addresses all four of the security challenges mentioned above by providing broad visibility and control of an organization's entire digital attack surface to minimize risk. The Security Fabric is an integrated solution that reduces the complexity created by supporting multiple point products, and automates workflow to increase the speed of operation—all while keeping business operations productive and resilient.

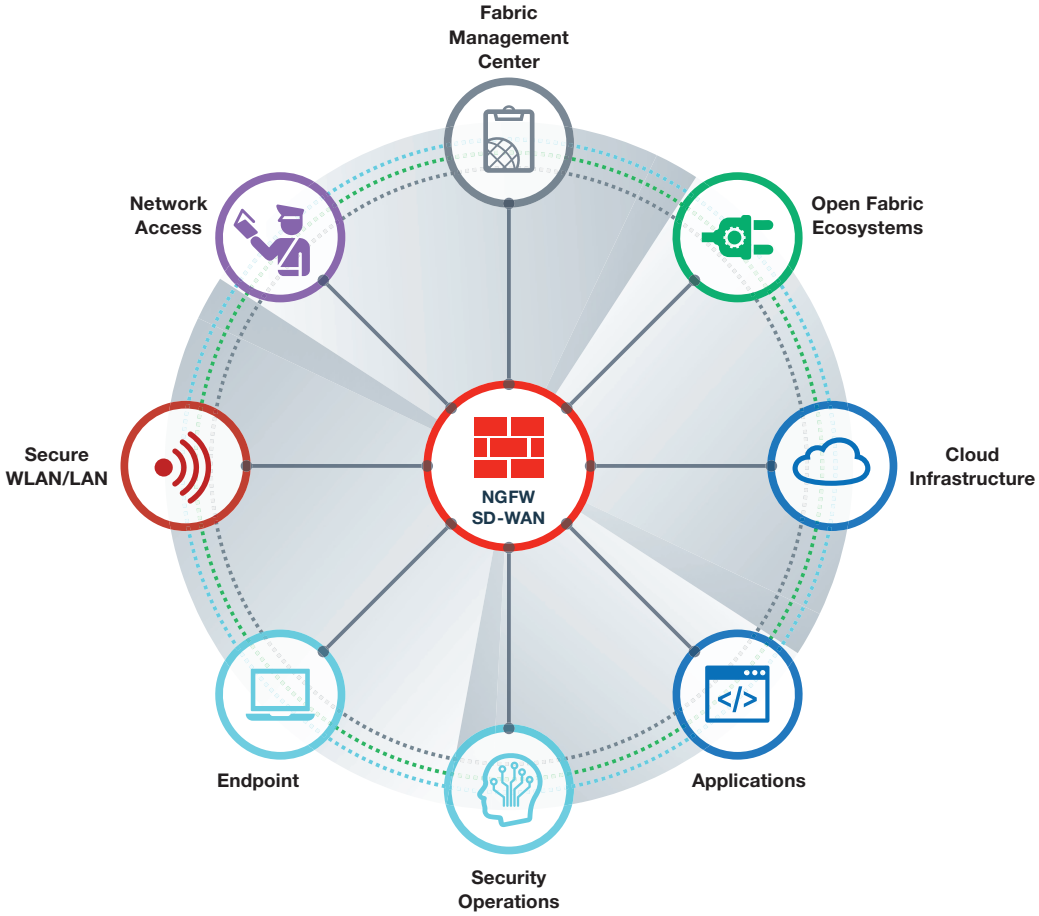


Figure 1: The Fortinet Security Fabric enables multiple security technologies to work seamlessly together, across all environments and supported by a single source of threat intelligence, under a single console. This eliminates security gaps in the network and hastens responses to attacks and breaches.

Almost half of CISOs point to security integration and improved analytics as a major priority for their cybersecurity technology strategy.[26]

With the Fortinet Security Fabric, teams can achieve:

Broad and deep attack surface visibility

With the broadest range of high-performance, security-driven networking solutions for data centers, branch offices and small business, and all major cloud providers, the Fortinet Security Fabric flexes to protect every segment of the network. All components are configured, managed, and monitored from a single centralized management system. In addition to eliminating the silos associated with point product security infrastructures, the single interface for all security components reduces the training burden on lean staffs. The management system also facilitates zero-touch deployment of remote components, saving truck rolls and further reducing operating costs.

A truly integrated security architecture

With all components driven by the same FortiOS network operating system, the Fortinet Security Fabric enables consistent configuration and policy management and effortless, real-time communication across the security infrastructure. This minimizes threat detection and mitigation times, reduces security risks resulting from configuration errors and manual data compilation, and facilitates timely and accurate compliance audit response. In addition to integrating Fortinet products and solutions, the Security Fabric includes prebuilt application programming interface (API) connections for more than 70 Fabric-Ready Partners that ensure deep integration across all of the Security Fabric elements.

FortiGate NGFWs provide the highest price-performance ratio in third-party evaluations while scanning encrypted traffic. They achieve 5.7 Gbps SSL performance while blocking 100% of evasions.[27]

Driving down breach detection and response time can result in a 25% reduction in the overall costs of a data breach.[28]

Automated operations and response

In addition to seamless integration, the Fortinet Security Fabric is leading the industry in applying machine-learning (ML) technologies to keep up with the rapidly evolving cyber-threat landscape. The Fortinet Security Fabric includes advanced security orchestration, automation, and response (SOAR) capabilities, as well as proactive threat detection, threat correlation, intelligence-sharing alerts, and threat research and analysis.

For network operations, the Security Fabric delivers automated workflows and operations to help reduce complexities across the organization, and across deployments regardless of whether it is on-premises, in the cloud, or at branches.

Manage the Risks, Pursue the Opportunities

DI enables organizations to achieve new levels of efficiency and cost savings for themselves and improved experiences for their customers. However, DI initiatives also expand and change organizations' attack surface, opening up new attack vectors for cyber threats to exploit.

For organizations leading the charge in DI, acknowledging, accepting, and properly managing risks is of paramount importance. The Fortinet Security Fabric is the foundation for this. It unifies security solutions behind a single pane of glass, makes the growing digital attack surface visible, integrates AI-driven breach prevention, and automates operations, orchestration, and response. In sum, it enables organizations to create new value with DI without compromising security for business agility, performance, and simplicity.

[1] Nick Lansing, "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources," Forbes and Fortinet, 2019.

[2] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[3] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, 2019.

[4] Ibid.

[5] Gilad David Maayan, "The IoT Rundown For 2020: Stats, Risks, and Solutions," Security Today, January 13, 2020.

[6] "Rightscale 2019 State of the Cloud Report," Flexera, 2019.

[7] Larry Ponemon, "Third-party IoT risk: companies don't know what they don't know," ponemonsullivanreport.com, accessed February 4, 2020.

[8] Nirav Shah, "SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019," Fortinet, September 9, 2019.

[9] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, 2019.

[10] "2019 Cost of a Data Breach Report," IBM Security and Ponemon Institute, 2019.

[11] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[12] According to internal data from FortiGuard Labs.

[13] "6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders," Fortinet, September 8, 2019.

[14] According to internal data from FortiGuard Labs.

[15] Kelly Bissell, et al.,"The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, 2019.

[16] "2019 Cost of a Data Breach Report," IBM Security and Ponemon Institute, 2019.

[17] Based off of internal Fortinet research.

[18] According to data from internal Fortinet research.

[19] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[20] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO, March 14, 2016.

[21] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[22] "Strategies for Building and Growing Strong Cybersecurity Teams: $(ISC)^2$ Cybersecurity Workforce Study, 2019," $(ISC)^2$, 2019.

[23] "CIO Survey 2019: A Changing Perspective," Harvey Nash and KPMG, 2019.

[24] "2019 Payment Security Report," Verizon, 2019.

[25] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, 2019.

[26] "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources," Forbes and Fortinet, 2019.

[27] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, January 2020.

[28] "2019 Cost of a Data Breach Report," IBM Security and Ponemon Institute, 2019.

www.fortinet.com

664959-0-0-EN

May 19, 2020 9:15 AM

ebook-considerations-security-architect