FORTINET

WHITE PAPER

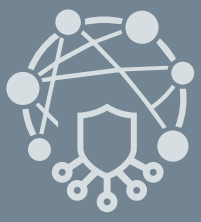
Fortinet Security Fabric Powers Digital Transformation

Broad, Integrated, and Automated

Executive Overview

DX offers new business advantages, and organizations are rapidly adopting digital technologies to accelerate their business, deliver better customer experiences, lower costs, and improve efficiencies. Organizations are migrating workloads and applications to the cloud, resulting in an explosion of IoT devices across multiple environments, and expanding business presence across markets and geographies.

But DX also introduces security challenges that pose serious risk to organizations—whether an expanded attack surface, an evolving advanced threat landscape, or increased complexity. The Fortinet Security Fabric solves these challenges by offering broad visibility of the entire digital attack surface, integrating AI-driven breach prevention, and automating operations, orchestration, and response.



78% of CIOs believe their digital strategy is only moderately effective—or worse.[1]

Introduction

Driven by the desire to move faster at global scale and to transform customer experiences, companies are reconsidering how they run their businesses—and digital transformation (DX) is at the forefront. Despite the wide-ranging business advantages DX offers, it also comes with new challenges. Specifically, as DX touches myriad technological aspects and extends from the data center and enterprise campus to the edges of the network and cloud, the network perimeter essentially dissolves, exposing additional risks while ratcheting up the complexity of an already-complex security architecture.

Applications can now live anywhere, and employees can work from anywhere at any time. This expanded attack surface makes traditional means for managing and securing a defined network perimeter ineffective. And as network and security leaders throw additional security products at the expanded attack surface, each increases the complexities of managing risk and compliance. Attacks are increasing in volume, velocity, and sophistication and becoming hard to detect and protect against.

Digital Transformation Seeds New Business Issues

For IT and cybersecurity leaders, DX initiatives create business changes that result in new technological realities. These roughly fall into three core areas:

Migration of workloads and applications to the cloud

Almost every enterprise is evaluating and/or undergoing workload and application migration to cloud-based deployments. The drivers for this are often the desire to reduce costs and to move faster in an ever-demanding business environment. This can happen either through Software-as-a-Service (SaaS) applications (e.g., Salesforce, Box) or by lifting-and-shifting applications that once resided in on-premises data centers to Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) models such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

Some organizations may strive for complete migration of all applications and services to the public cloud over the next few years. More commonly, businesses are electing to be more discriminating over what actually gets migrated and on which platform—embracing a hybrid cloud strategy that includes both private (on-premises) and public clouds. However, in addition to expanding the attack surface, these multi-cloud environments reside in silos and create complexity. They also increase risk exposure due to misconfiguration of SaaS applications or cloud infrastructure and platforms.

Explosion of IoT devices across multiple environments

Internet-of-Things (IoT) devices continue to multiply across enterprise environments. Though estimates vary, most analysts predict upwards of 30 billion devices will be in use within the next year.[3] The business possibilities of IoT are immense, and many believe we are still in the early phases of IoT innovation and adoption.

The list of IoT devices is extensive—everything from light switches, to printers, to medical devices, to ATMs. Yet, when it comes to security, these connected devices present significant challenges due to their lack of built-in security features. They have limited resource footprints, which means that traditional endpoint security solutions are too large or resource-intensive to run on many IoT devices. Further, while IoT devices typically reside on the edges of the network, they transmit and store critical information shared with on-premises and cloud services.

Expanded business presence across distributed markets and geographies

Businesses are becoming increasingly distributed, with branch network traffic volumes growing exponentially due to SaaS applications, video, and Voice over IP (VoIP). This offers opportunities for increased productivity and collaboration and even reduced costs. However, geographically distributed network environments have limited control and visibility of the users, machines, and devices located in remote locations. Because branches also connect back to the central campus and often share the same systems and applications, performance and availability compromises at a single location can have a domino effect across the entire organization.

For enterprises that have embraced software-defined wide-area networks (SD-WAN), which no longer route traffic through the data center but over public internet connections, security implications can be quite serious. Further, while the network traffic is no longer tethered to MPLS connections and data-center availability and scalability, application performance assumes a different dynamic with SD-WAN.

83% of enterprise workloads will be in the cloud by 2020, and 63% of IT professionals see security as the most significant concern about this trend.[2]

Cyber criminals have IoT devices and their vulnerabilities squarely in their sights. An estimated 25% of all attacks will target IoT devices by 2020.[4]

A key feature of SD-WAN is its ability to deliver the cost-performance benefits of internet-based VPNs with the performance and agility of MPLS VPNs.[5]

Three Challenges Facing Security Leaders

The above business dynamics translate into three key security challenges:

Expanding attack surface

Sensitive data can now reside across multiple clouds and within reach of a growing array of deployed IoT devices. Traffic moves across the public internet instead of private networks and extends to the edges of the network—from mobile devices and wireless access points to operational technology (OT). This expanded, dynamic attack surface dissolves the once well-defined network perimeter and the security protections associated with it.

Seeking to address the new vulnerabilities posed by this new network reality, many organizations have deployed an array of largely disaggregated point security products. Over three-quarters of organizations admit their security architectures are disjointed due to nonintegrated security products.[6] This de facto security architecture is disconnected, engendering multiple security and compliance gaps and inefficiencies that, ironically, diminish holistic protection.

Disaggregated security also wastes staff resources by requiring manual workflows and administration. Worst of all, this increases risk to organizations. Distractions from strategic priorities are frequent, with security incidents requiring an "all-hands-on-deck" approach to remediation.[7] As a result, security teams find themselves in a perpetual reactive mode with regard to current threats, which leaves them unable to plan and anticipate the attacks to come in the near future.

Advanced threat landscape

The volume and velocity of threats continues to explode. For example, unique exploits grew 5% and exploits detected per firm increased 10% in this past quarter.[9] There are many reasons for this explosive growth, starting with the fact that the bar for accessing malware is lower than ever due to the availability of Malware-as-a-Service (MaaS) and other on-demand services on the darknet.

Advanced threats are becoming more sophisticated at the same time. Many are now multi-vector, concurrently targeting different points on the expanded attack surface in coordination. All at once, an attack can blitz an organization from a central data center out to the network edge, targeting a full spectrum of endpoint devices and applications across on-premises and cloud environments. Some exploits have become "living organisms" that employ polymorphic malware to circumvent the latest signatures and patches.[10]

These advancements are also making it more difficult to detect and respond to breaches. For example, over the last year, the mean time to identify a data breach incident increased from 191 days to 197 days, an indication that greater sophistication is making threats harder to detect.[11] And it is no longer just about detection and protection. Cyber resiliency—the ability to quickly mitigate and remediate a breach—is critically important, with four out of five organizations reporting at least one intrusion in the past year.[12]

Greater complexity

The breadth of point security products and the growing disaggregation of the security architecture is increasing the complexity of security management for enterprises. Upwards of 75 different security solutions are used by the average enterprise, many of which address a single new element of the attack surface or compliance requirement.[14] In this largely disaggregated security architecture, these different solutions typically do not communicate with each other.

New and evolving industry and government regulations such as the European Union's General Data Protection Regulation (GDPR) and adoption of security standards such as the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework further complicate the picture for IT and security leaders. Business growth through mergers and acquisitions as well as flexible operations arrangements with contractors and service providers also create additional layers of business complexity—and vulnerabilities in terms of device and user access management.

The increased complexity resulting from these different issues is stretching overburdened cybersecurity teams. Hiring additional staff to manage the resulting manual work processes cannot be solved by adding more headcount. Indeed, finding and retaining cybersecurity professionals with the right skill sets has never been more difficult, with nearly 3 million unfilled security positions worldwide today—a number that is expected to grow in coming years.[15]

Nearly 80% of organizations are introducing digital innovations faster than their ability to secure them against cyberattacks.[8]

Up to 40% of new malware detected on a given day is now zero-day or previously unknown.[13]

65% of CIOs express that a lack of cybersecurity talent is holding their organizations back.[16]

The Fortinet Security Fabric

The Fortinet Security Fabric addresses the three aforementioned security challenges by providing broad visibility of the entire digital attack surface, integrated AI-driven breach prevention, and automated operations, orchestration, and response.

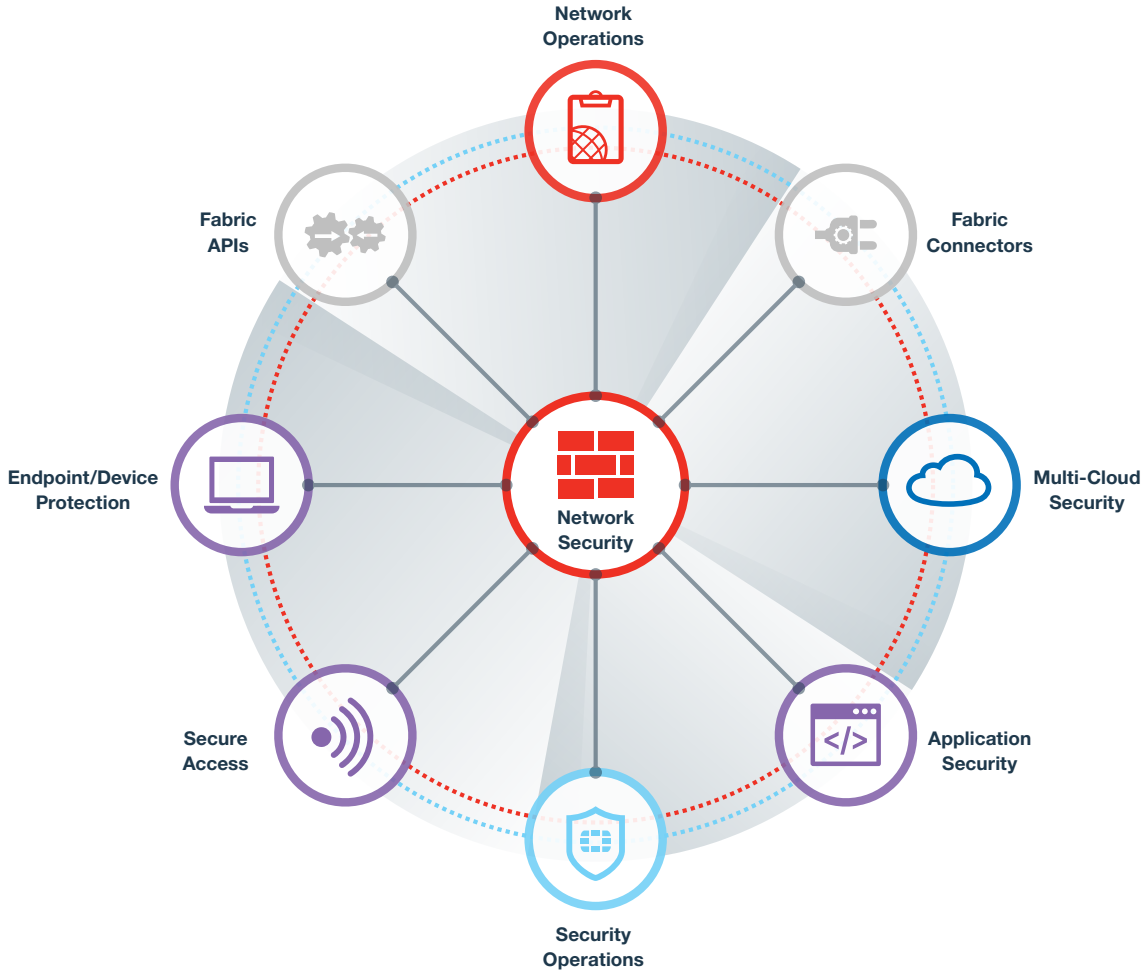


Figure 1: The Fortinet Security Fabric.

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

Integrated across the Security Fabric, Fortinet Intent-based Segmentation continuously monitors the trust level of users, devices, and applications and dynamically controls access based on business intent, behavior, and risk. This dramatically shrinks the attack surface by making it more difficult for intruders to find vulnerabilities and to exploit them by preventing their lateral (east-west) movement across the network.

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. Additionally, for security products that are not part of the Fabric-Ready Partner ecosystem, REST APIs and DevOps scripts make it easy and fast for customers to add them to the Security Fabric.

Effective segmentation must leverage business intent to establish where, how, and what for effective security execution.

Integrated, AI-driven breach prevention

Because the Security Fabric fully integrates the entire attack surface and each security element, it can also share global threat intelligence from FortiGuard Labs on newly detected zero-day attacks, advanced threats, botnets, indicators of compromise (IOCs), and more.[17]

To detect threats, FortiGate NGFWs scan encrypted secure sockets layer (SSL)/transport layer security (TLS) traffic. As encrypted traffic now makes up 72% of all network traffic and hides 50% of cyberattacks, inspection of encrypted traffic is a nonnegotiable.[18, 19] Unlike other firewall solutions that experience dramatic performance impact, FortiGate NGFWs use purpose-built security processors (SPUs) to minimize performance degradation, which enables organizations to avoid retrofitting and adding more appliances to their firewall infrastructure—whether in the data center or on the edges of the network.

The volume and velocity of malicious attacks, coupled with their increasing sophistication, makes it difficult for cybersecurity defenses to keep pace. Blocking known threats is not enough today. More than three-quarters of successful attacks leverage unknown or polymorphic malware or zero-day attacks.[21] Artificial intelligence (AI) and machine learning (ML) offer organizations the means stay ahead of cyber criminals. Unfortunately, only slightly more than one-third of security vendors use AI and ML capabilities in their solutions.

Fortinet recognized the importance of doing so years ago in its development of FortiGuard AI. Specifically, FortiGuard Labs uses AI-driven capabilities, including ML, that leverage 4.4 million sensors around the world and partnerships with over 200 global organizations. This AI/ML-driven threat intelligence uses 5 billion nodes to identify unique malicious or clean features for both known and unknown threats. In all, FortiGuard Labs processes more than 100 billion web queries every day and blocks 2,600 malicious URLs every second.[22] Fortinet AI/ML capabilities are also integrated into FortiWeb and FortiInsight, enabling organizations to dramatically reduce false positives in the case of FortiWeb and to use forensics analysis at the user, system, and network layers to detect and prevent insider threats in the case of FortiInsight.

Other capabilities such as sandboxing and the use of decoys also play a critical role in stopping advanced threats before they impact operations or result in a data breach. Specifically, both FortiSandbox[23] and FortiDeceptor[24] are fully integrated into the Security Fabric, enabling them to automatically share their threat intelligence in real time across all of the security elements.

Automated operations, orchestration, and response

The influx and speed of DX projects makes it harder for organizations to protect against advanced threats. Almost 80% of organizations admit they are introducing DX at a pace faster than their ability to secure them from cyberattacks.[26] Add new and evolving regulations and the adoption of security standards, along with the fact that threats are faster and more advanced than ever, and the complexity of security expands exponentially.

Automated workflows and orchestration—from detection, to protection, to response—becomes a requirement for any enterprise seeking to succeed in this complex world of security management. This is where the Security Fabric delivers tangible dividends.

Automation of network operations helps DevOps teams to focus on time to market, improves operational efficiencies through zero-touch provisioning, and generates real-time insights around branch network performance around issues such as spikes, scaling, and priority routing of traffic. Automation of security operations reduces risk through proactive threat detection, threat correlation, intelligence-sharing alerts, and threat research and analysis.

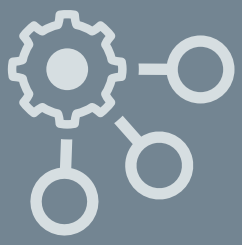
FortiGate NGFWs deliver the leading price-performance ratio in competitive tests when scanning encrypted traffic. Results include blocking 100% of evasions.[20]

Automation, artificial intelligence, and machine learning are only being taken up by 38% of organizations. This not only represents a lost opportunity but also exposes organizations to advanced threats that traditional security models cannot address—or keep up with.[25]

77% of organizations rely on nonintegrated point security products to some degree within their organization—leaving gaps in security effectiveness.[27]

With successful intrusion and breaches inevitable, cyber resiliency is receiving increased attention.[28] Integration of IT service management (ITSM) tools unlocks automation of event analysis and responses. This reduces response times from days to minutes or even seconds.

The Security Fabric also uses automation to transform compliance audits, tracking, and ongoing reporting across industry regulations and security standards. The latter includes dashboards for the CISO, CIO, CEO, and even the board of directors. This saves security teams myriad hours in manual log aggregation and correlation, a task that is particularly onerous with a disaggregated security architecture lacking transparent visibility and centralized controls.



Automation of security workflows and threat intelligence also enables overstretched security teams to do more with their existing skill sets and resources.

Security Fabric Solution Elements

The Security Fabric contains eight different solution areas. Each of these includes best-in-class, award-winning solutions that are backed by leading independent tests such as NSS Labs and recognized by leading analysts such as Gartner.[29, 30]

Network Security

Network security

Network security extends from the data center and enterprise campus to the edges of the network. Some of the core capabilities comprising network security include:

SD-WAN architectures can help distributed organizations achieve faster connectivity, cost savings, and improved cloud application performance versus traditional WAN environments. FortiGate NGFWs include Fortinet Secure SD-WAN, which combines branch networking and firewall security in a single, unified solution. In combination with FortiManager, Fortinet Secure SD-WAN supports application visibility and control, high-quality voice and video delivery, and consolidated management of networking and security for branch networks. Fortinet SD-Branch integrates Secure SD-WAN capabilities into the local area network (LAN) and extends security into the access layer.

NGFWs simplify security complexity and provide visibility into applications, users, and networks. FortiGate NGFWs utilize purpose-built security processors and threat-intelligence services from FortiGuard Labs to deliver top-rated security and high-performance threat protection (e.g., intrusion prevention, web filtering, anti-malware, application control). FortiGate NGFW automated, policy-based responses accelerate time to resolution.

Intent-based segmentation efficiently translates business intent into fine-grained access control that is adjusted based on the continuous trust assessment of users, devices, and applications. Deep integration across Fortinet Security Fabric solutions enables intent-based segmentation that improves an organization's defensive posture, mitigates risks, supports compliance, and boosts operational efficiencies.

Management and analytics tools enable security teams to do more with limited security resources. Fortinet Management and Analytics solutions (e.g., FortiAnalyzer, FortiCloud, FortiManager, FortiSIEM) provide efficient administration, transparent visibility, and intelligence and real-time insights across the entire Security Fabric. They simplify management workflows, shorten deployment times, and reduce the chances of misconfiguration caused by human errors.

Cloud Security

Cloud security

Fortinet solutions for cloud security provide superior visibility, protection, and control across public, private, SaaS, and hybrid cloud environments. Fortinet Cloud Security offers single-pane-of-glass visibility and unified security across multiple cloud deployments. Core solution areas include:

Seamless **visibility and control** for public clouds is powered by FortiCASB cloud access security broker (CASB) for the monitoring and configuration of cloud deployments and SaaS applications. FortiGate-VM provides advanced protection for north-south traffic in a virtualized environment such as a private cloud or software-defined data center (SDDC). It enables centralized visibility and control and full automation of security processes in concert with other security elements within the Security Fabric. FortiGate-VM also enables deep-packet inspection—both of encrypted and nonencrypted traffic—of east-west application and user traffic moving between virtual machines. FortiSIEM, FortiManager, and FortiAnalyzer offer cloud insights through management and analytics capabilities while delivering comprehensive cloud compliance tracking and reporting.

Application security for cloud deployments taps microsegmentation, using FortiGate-VM, to isolate workloads from one another and secure them individually—restricting lateral (east-west) movement of malicious intrusions. Fortinet also offers security that can be integrated into the container application life cycle. FortiGate-VM connects to the container management layer and learns the labels of different containers. FortiWeb serves as a container image that allows developers to roll out security controls alongside their application development life cycle and to port application security along with other application services throughout the application life cycle. FortiSandbox-VM mitigates the risk introduced through agile development methodologies by integrating into application containers.

Secure connectivity enables high-speed VPN capabilities for secure data transfers across hybrid infrastructures. Facilitated by the Security Fabric, organizations have transparent visibility, unified controls, and centralized enforcement of policies across all cloud environments. They also can provision preconfigured instances of FortiGate-VM globally across all clouds and have always-on connectivity to business applications through the closest entry point on the network.

Application Security

Application security

Attacks that target applications require additional protections that a firewall or an intrusion prevention system (IPS) cannot provide. Organizations need web application firewalls, application delivery controllers, and sandboxing to address the latest threats. Within the Security Fabric, web-based applications receive more protection than if point security products were used.

Web application solutions provide unified security to mitigate the risks inherent to cloud-based applications. This enables the Security Fabric to streamline the protection of vulnerable systems and gain deep visibility of web-based, publicly facing applications. Fortinet also supports compliance for regulated applications, including templates to simplify ongoing regulatory needs and operations—such as for the Payment Card Industry Data Security Standard (PCI DSS).

Email requires dedicated advanced threat detection. The Security Fabric includes solutions for securing cloud-based email via SaaS, public cloud, or API-based deployment (complementing the built-in capabilities of Microsoft Office 365 or Google G Suite). This includes consolidated email security via a comprehensive Secure Email Gateway (SEG) offering.

Security Operations

Security operations

The Security Fabric brings in context from network elements beyond the Fortinet family of products (i.e., preexisting infrastructure) to enhance security operations. This provides organizations with comprehensive protection that covers both IT and security risk management across the entire enterprise. FortiSIEM, FortiAnalyzer, and FortiManager as well as FortiGuard threat intelligence data collectively address these needs.

Prevent cyber threats by keeping pace with the evolving threat landscape. Curated threat-intelligence feeds for things like malicious files and IP addresses help stop attacks well in advance. Consolidated security across multiple disciplines using FortiAnalyzer shares intelligence in real time for coordinated, lockdown defensive responses.

Advanced threat detection capabilities powered by FortiGuard Labs spot threats like new malware variants. Available in all form factors, FortiSandbox integrates with all elements of the Security Fabric and enables organizations to identify known and unknown threats before they impact the business. FortiDeceptor deploys decoys used to analyze threat activity and share information across the Security Fabric.

Automated responses to security incidents shrink the time to resolution for detection, protection, and remediation. Security Fabric automation capabilities include flexible workflows that combine policy-based event triggers, response actions, and approvals to quickly contain threats.

Compliance support in the Security Fabric includes out-of-the-box reporting for PCI DSS and other regulatory controls that reduce the reporting and auditing burdens for under-resourced security teams. The Security Fabric also facilitates automated assessment of controls against NIST, CIS, and other security best practices. It also provides quantified risk scoring, both internally over time and against similar organizations through the Security Rating Service.

Training support includes public modules for employees and executives focused on threats, security technologies, and solutions. Technical training is provided via an official eight-level Network Security Expert certification program covering Fortinet products and solutions.

Secure Access

Secure access

Enterprises with distributed branch locations face complexity in a world of multi- and hybrid-cloud deployments. Organizations are rapidly adopting technologies such as SD-WAN to address performance issues by enabling network traffic over the public internet. But this type of traffic carries risk, and it is imperative that next-generation security strategies be integrated into multi-path WAN deployments.

The Fortinet SD-Branch solution integrates Fortinet Secure SD-WAN with the LAN at each branch location and includes common management tools on a single pane of glass. With SD-Branch, organizations have improved visibility at the branch and corporate levels and can enable security and networking processes. The result is that security is extended to the access layer and global security policies can be applied automatically at the branch level.

User, Endpoint, and Access

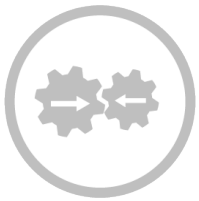
User, endpoint, and access

The Fortinet Security Fabric also supports comprehensive security for devices and end-users. These capabilities include:

FortiClient provides advanced threat protection against exploits and advanced malware, powered by threat intelligence from FortiGuard Labs, to protect a growing array of **IoT devices** that often lack built-in security. FortiClient can be integrated with other Security Fabric solutions like FortiSandbox using Fabric Connectors, providing protection against known and unknown threats. FortiClient also provides a vulnerability dashboard that helps administrators manage the attack surface and perform on-demand vulnerability scans.

Endpoint visibility and protection means that an administrator has a comprehensive view of every device connected to the network. The endpoint telemetry and compliance license for FortiGate NGFWs provides a unified view for all Security Fabric elements, enabling centralized enforcement of endpoint security policies.

Identity and access management with FortiAuthenticator supports intent-based segmentation by centralizing user identity information, helping organizations to provide the right access to the right person at the right time—securely. Fortinet Single Sign-On (SSO) enables this protection to be seamless for the end-user. Two-factor authentication is enabled by FortiToken, which leverages FortiGate NGFWs as their authentication server for a scalable, low-entry cost, and low total cost of ownership (TCO) solution. And with FortiInsight user and entity behavior analytics (UEBA), organizations can bolster protection against insider threats by detecting behavioral anomalies that might signal a threat.



Fabric API

Fabric Connectors

Open ecosystem

The open ecosystem of the Fortinet Security Fabric unifies security solutions, enabling them to communicate and work together. Integration encompasses the following elements:

The **Fabric API** enables technology providers to develop integrations for their products with the Fortinet Security Fabric. Dozens of Fabric-Ready Partners span a broad range of technologies, enabling organizations to have integrated, unified protection for an ever-expanding attack surface. For core technology areas, customers can leverage Fortinet-validated integrations or joint solutions with partners.

Fabric Connectors enable deeper, API-based integration for various platforms in an organization's ecosystem, enabling them to connect seamlessly with the Fortinet Security Fabric. They are easily deployed with a simple click on the GUI and do not require hardware or software modifications to existing systems. Fabric Connectors enable automated, consistent security protection across a complex hybrid environment.

DevOps Scripts automate Fortinet security provisioning and configuration management using the open architecture of the Fortinet Security Fabric. Different scripts have been developed by Fortinet, its partners, and its customers to help organizations to connect disparate security solutions into the unified Fabric framework. They help organizations keep up with rapid changes in both the IT infrastructure and the threat landscape. DevOps scripts are easily executed and can be found on the Fortinet Developer Network and on GitHub.

Network Operations

Network operations

The Fortinet Security Fabric enables smooth network operations, enabling the network operations center (NOC) to share the same management console with the security operations center (SOC).

Single-pane-of-glass management means that all network operations are monitored centrally, with zero-touch provisioning of new resources to reduce complexity. Configurations are also managed centrally for all devices—and revisions are backed up. And administrators have full, centralized control with out-of-the-box workflows and scripts and Fortinet open API for organization-specific needs.

Best-practice compliance enables organizations to not only comply with regulations and standards but also manage risk according to risk tolerance that may differ from the compliance requirements. The Security Rating Service provides an objective risk score against accepted benchmarks and peer organizations, with actionable advice on how to achieve a better risk management posture. FortiManager helps organizations track policy changes across the network and who made them, and helps address complexity by eliminating and consolidating unused policies.

Automation and orchestration optimize operations across the enterprise. Workflow optimization provides policy change workflow controls to limit users' ability to change policies in ways adverse to security. Fabric-Ready workflow tool integrations streamline operations and reduce risk. And for the DevOps environment, organizations can deploy turnkey management with scripts and playbooks for their continuous integration (CI)/continuous delivery (CD) integrations.

Manage the Risks, Pursue the Opportunities

DX is an opportunity for nearly every organization to achieve more flexibility and cost efficiency for itself and better experiences for its customers. At the same time, DX increases the digital attack surface, gives hackers innovative ways to generate increasingly sophisticated attacks, and contributes to a growing complexity of regulations and security solutions.

This will not stop emerging leaders—the ones who build a foundation for managing risk that enables their organizations to move faster than competitors in leveraging DX. The Fortinet Security Fabric is that foundation. 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 DX without compromising security for business agility, performance, and simplicity.

[1] "CIO Survey 2018: The Transformational CIO," Harvey Nash and KPMG, May 25, 2018.

[2] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud by 2020," Forbes, January 7, 2018.

[3] "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," Statista, accessed March 20, 2019.

[4] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed March 21, 2019.

[5] Zeus Kerravala, "Understanding Virtual Private Networks [and why VPNs are important to SD-WAN]," Network World, April 13, 2018.

[6] "State of the CIO and Security Report," Fortinet, April 2019.

[7] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[8] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon, March 6, 2019.

[9] "Quarterly Threat Landscape Report: Q4 2018," Fortinet, February 2019.

[10] Kevin Williams, "Threat Spotlight: Advanced polymorphic malware," SmarterMSP.com, June 13, 2018.

[11] "2018 Cost of a Data Breach Study," Ponemon, July 2018.

[12] "The CISO and the State of Cybersecurity Report," Fortinet, April 2019.

[13] According to internal data from FortiGuard Labs.

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

[15] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," $(ISC)^2$, October 18, 2018.

[16] "CIO Survey 2018: The Transformational CIO," Harvey Nash and KPMG, May 25, 2018.

[17] "FortiGuard Labs," Fortinet, accessed March 22, 2019.

[18] John Maddison, "Encrypted Traffic Reaches A New Threshold," Network Computing, November 28, 2018.

[19] "Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity," Lifeline Data Centers, accessed March 21, 2019.

[20] "Fortinet Receives Recommended Rating in Latest NSS Labs NGFW Report, Delivers High SSL Performance Suited for Encrypted Cloud Access," Fortinet, July 17, 2018.

[21] Charlie Osborne, "Zero-days, fileless attacks are now the most dangerous threats to the enterprise," ZDNet, October 16, 2018.

[22] "Threat Intelligence with Integrated AI and ML Reduces Risk and Supports Performance," Fortinet, September 29, 2018.

[23] "Mapping the Requirements of Next-Generation Sandboxing to Address the Advanced Threat Landscape," Fortinet, June 13, 2018.

[24] "FortiDeceptor Enables a New Breach Protection Approach," Fortinet, *forthcoming*.

[25] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon, March 6, 2019.

[26] Ibid.

[27] Patrick E. Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar Security Blog Post, February 20, 2019.

[28] "State of the CIO and Security Report," Fortinet, April 2019.

[29] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, January 2019.

[30] "2018 Gartner Magic Quadrant Reports," Fortinet, accessed March 21, 2019.

March 29, 2019 11:44 AM

381915-0-0-EN

Macintosh HD:Users:bhoulihan:Documents:_Projects:White Paper:wp - Security Fabric:rounds:wp-security-fabric-032919-1200pm