SOLUTION BRIEF

FortiOS: Enabling the Fortinet Security Fabric

Executive Summary

Organizations worldwide continue to adopt new technologies to keep up with the growing pace of digital transformation (DX). While DX unlocks new possibilities, it also expands the attack surface, resulting in a patchwork of point security solutions that creates a fragmented network that does not communicate.

FortiOS, the Fortinet security operating system, enables the Security Fabric to connect security devices across the entire networking infrastructure to deliver effective protection with a single, adaptive operating system. The latest release of FortiOS includes hundreds of new capabilities that create deeper visibility and control across the breadth of the entire attack surface, integrate artificial intelligence (AI)-driven breach prevention throughout the network for seamless protection and threat detection, and automate operations, orchestration, and response.

In addition to an acute shortage of skilled staff and limited budgets, today's enterprise security leaders face growing complexity everywhere they turn—from increasingly sophisticated cyber threats, to an expanding collection of disparate security products staggered across their networks, to new demands for compliance from regulation and security standards. The drive for DX across all areas of a business requires networks to evolve rapidly, calling for applications, data, and services to flow faster across an increasingly diverse landscape of users, domains, and devices. Plus, Internet-of-Things (IoT) devices and cloud infrastructure now require organizations to worry about an attack surface that may not even be visible to IT.

Security Fabric Approach

There are approaches that attempt to use multiple point and platform solutions to address these challenges. But what if all the data and security elements across an organization's various environments could be tightly integrated, cohesive, and coherent—like a seamlessly woven fabric? Such an approach would allow companies to see, control, integrate, and manage security across their entire infrastructure from network to cloud, enabling a secure digital business model. This approach would also allow security to dynamically expand and adapt as more workloads and data are added, while at the same time easily follow and protect data, users, and applications as they move back and forth between smart devices, borderless networks, and cloud-based environments.

The Fortinet Security Fabric provides a more effective alternative to point and platform solutions. All security components within the Security Fabric are made available to each other in real time to provide broad, integrated, and automated protection against sophisticated threats. The FortiOS network operating system provides the foundation to establish and enable the Security Fabric. The latest release—FortiOS 6.2—includes more than 300 new features and capabilities that are designed to help enterprises embrace DX without impacting network performance or compromising security.

An estimated 25% of all attacks will target IoT devices by 2020.[1]

83% of enterprise workloads will be in the cloud by 2020.[2]

300 new capabilities to unlock secure DX with FortiOS 6.2.

Over three-quarters of enterprises admit that they are introducing digital innovations faster than their ability to secure them against cyberattacks.[3]

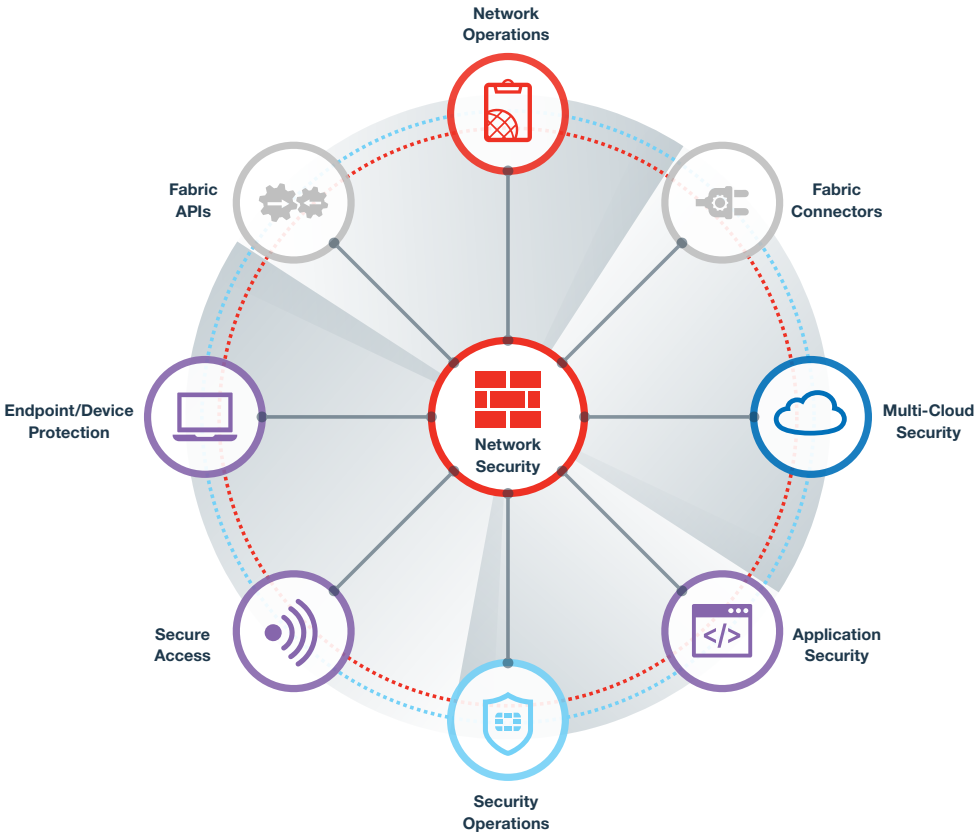

Figure 1: The Fortinet Security Fabric.

Broad: Visibility of the Entire Digital Attack Surface

To protect today's businesses, security solutions cannot stand alone as isolated devices scattered across the network. The Security Fabric covers the entire attack surface in order to stop the impact of a threat at multiple points. To help achieve this, FortiOS 6.2 enables greater visibility and control across the entire environment—including endpoints, access points, network elements, the data center, the cloud, and even the applications and the data itself. Combined with intent-based segmentation that logically separates data and resources, the Security Fabric covers all attack vectors to discover threats and contain them as they attempt to move from one network zone to the next. This enables organizations to protect their network and data.

Expanded native cloud and virtual connectors within the Security Fabric enable full visibility across multi-cloud environments, including private, Infrastructure-as-a-Service (IaaS), and native cloud controls. FortiCASB-SaaS (cloud access security broker) also provides visibility and advanced threat protection of Software-as-a-service (SaaS) applications. Multi-cloud visibility can help organizations correlate both on- and off-network traffic through a single security management console.

FortiOS 6.2 also supports integrated Fortinet Secure SD-WAN within the Security Fabric, providing application prioritization for granular control of SaaS, Voice over IP (VoIP), and other business-critical applications. Other new capabilities include traffic shaping to guarantee bandwidth for critical applications, zero-touch deployment for plug-and-play SD-WAN location management, and one-touch VPN to leverage common cloud VPN access. Additionally, FortiOS 6.2 offers customers the ability to benefit from capabilities designed to deliver quality of experience (QoE) to their users. With QoE, an organization's business never skips a beat, even if something in the environment does.

Integrated: AI-driven Breach Prevention

Security has become incredibly complex for many organizations. They continuously add more point products to cover new security gaps and exposures. This, in turn, compounds the ongoing resource strains of deployment, management, and oversight—many of which may be manual processes. New regulations are increasing compliance and reporting requirements. These complexity challenges are further exacerbated by a worldwide scarcity of skilled security professionals—especially skills in certain areas like cloud security, DevSecOps, and incident response, among others.[4,5]

To ensure comprehensive protection in the face of burgeoning complexity, all of the different parts of a company's security infrastructure must work together as a single, unified system. The Security Fabric is designed not only for integrated protection across all devices and systems securing the distributed network but also for rapid awareness of advanced threats. FortiOS 6.2 integrates many new intelligent features that enable precise threat-detection capabilities throughout the infrastructure. AI-driven intelligence is supplied from FortiGuard Labs and is collected across the Security Fabric. It is then shared throughout a cohesive, end-to-end security architecture, unlocking potential automation and reducing the impact of staffing shortages. As one of many examples, the Security Fabric can take automated action based on trusted analysis, streamline communications, and expedite patching without the limits of human monitoring and intervention.

Additionally, Fortinet continually delivers new, leading-edge technologies and capabilities into the Security Fabric, allowing it to scale and grow as needed. FortiOS 6.2 delivers native transport layer security (TLS) 1.3 support for a seamless, secure internet traffic experience and deception-based security through FortiDeceptor, enabling organizations to detect active intrusions and active bad actors.

Automated: Operations, Orchestration, and Response

Integration and automation go hand in hand. Once a threat is detected, the response time to a security event must be instantaneous to minimize exposure. The Fortinet Security Fabric is designed to shrink the windows from both intrusion to detection and detection to response. The Security Fabric correlates threat intelligence to determine the level of risk and automatically synchronizes a coordinated response. It shares intelligence about newly discovered threats, dynamically isolates affected devices, partitions network segments, updates rules, pushes out new policies, and removes malware. And beyond reducing risk exposure, replacing manual security processes with automation also helps address the organizational challenges of tighter budgets and a skilled staffing shortage.

New Capabilities in the Security Fabric

Additionally, the Fortinet Security Fabric delivers a suite of capabilities designed to help reduce complexity holistically. This includes the ability to automate application inventory on each device and security responses to events across Fortinet switches and wireless access points. Automated workflow with continuous risk assessment allows users to easily set responses based on predefined triggers, such as system events, threat alerts, and user and device status. Responses (such as quarantine, notification, configuration adjustments) and custom reports provide real-time control of workflow environments. Automated auditing provides trending data on a business's security compliance posture with benchmarking that ranks organizations against similar firms in terms of size and industry.

Fortinet is also the only vendor to provide a true single pane of glass across all solutions within the infrastructure, from Fortinet's own solutions to the extensive ecosystem of partners and third-party solutions integrated into the Security Fabric. The single-pane-of-glass capability further simplifies operations and responses that go beyond automated policies and rules.

Other new features within FortiOS 6.2 support best practices for auditing and compliance to make it easier for businesses to adhere to and implement the latest standards and regulations, starting with the Payment Card Industry Data Security Standard (PCI DSS). FortiOS includes built-in rules that help enterprises avoid lengthy rule-creating processes that can be difficult to enforce and time-consuming to track.

FortiOS 6.2 Enables:

- Intent-based segmentation
- Secure SD-WAN
- End-user QoE
- AI-backed threat intelligence
- Deception-based security
- Automated response
- Audit and compliance best practices
- Single-pane-of-glass management

Advanced threat and breach detection is a requisite, with upwards of 40% of new malware detected on a given day now zero-day or previously unknown.[6]

Automation, artificial intelligence, and machine learning are only being taken up by 38% of organizations.[7]

Conclusion

DX raises multiple security challenges for an enterprise. Trends in computing and networking will continue to drive changes across business infrastructures, architectures, and practices, while cyber criminals continue to evolve new and better ways to exploit exposed vulnerabilities. As a critical part of these changes, business leaders must embrace a new approach to securing the entirety of their distributed infrastructures. The Fortinet Security Fabric provides an intelligent architecture designed around scalable, interconnected security combined with high awareness, actionable threat intelligence, and open API standards to protect even the most demanding enterprise environments.

FortiOS 6.2 is the latest version of the Fortinet network security operating system. With hundreds of enhancements and feature additions, it expands the Security Fabric with deeper visibility and control across the breadth of an organization's entire attack surface. It also delivers integrated AI-driven breach prevention throughout the network for seamless protection and threat detection, as well as automated operations, orchestration, and response that quickly identify and resolve security issues, while enabling organizations to reduce complexity and move faster.

[1] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed March 21, 2019.

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

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

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

[5] Dawn Kawamoto, "Top 8 Cybersecurity Skills IT Pros Need in 2018," Dark Reading, December 18, 2017.

[6] According to internal data from FortiGuard Labs.

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

March 28, 2019 11:02 AM

384970-0-0-EN

Macintosh HD:Users:bhoulihan:Documents:_Projects:Solution Brief:sb-FortiOS 6.2:rounds:sb-fortiOS-6.2-032819-1100am