SOLUTION BRIEF

Understanding FortiOS—The Heart of the Fortinet Security Fabric

Executive Summary

FortiOS, the Fortinet network operating system, is the heart of the Fortinet Security Fabric. This operating system, or software, is at the core of the Security Fabric and ties all components together to ensure a tight integration across an organization's entire Fabric deployment. With version 6.4, FortiOS adds new capabilities designed to support organizations' digital innovation (DI) goals. These include improved visibility of Internet-of-Things (IoT) devices, enhanced network access control (NAC) integration, improved endpoint protection, and added security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities.

Almost half of CISOs point to security integration and improved analytics as a major priority for their cybersecurity technology strategy.[1]

Nearly 80% of organizations are introducing innovations faster than their ability to secure them against cyberattacks.[2]

84% of enterprises have a multi-cloud strategy. 81% point to security as a major cloud challenge.[3]

Fortinet Security Fabric Enhances Support for Digital Innovation

The Fortinet Security Fabric is a **broad, integrated**, **and automated** network security architecture that solves four primary challenges for the digitally innovating enterprise:

1. An expanding, fragmenting attack surface
2. Accelerating advanced threats
3. A profusion of disparate network security technologies
4. Increasingly onerous regulatory demands regarding network security and data privacy

The multilayer defense-in-depth strategies required to meet these challenges translate into numerous sophisticated and evolving security capabilities. Consequently, the Security Fabric includes a broad range of solutions, which can be deployed either as hardware appliances, as virtual machines, or as a hosted service. A central advantage of all these solutions is that they are integrated, orchestrated, and centrally managed from a single pane of glass, minimizing security gaps and operational complexity. And FortiOS is the key to enabling this seamless, integrated protection.

FortiOS Enables Broad, Integrated, Automated Security

FortiOS is the network operating system of the entire Fortinet Security Fabric. Every component—from the next-generation firewalls (NGFWs) to the access points and switches to the NAC solution—is driven by the same FortiOS code. This means that the Security Fabric components:

- Are configured and managed the same way, so network and security administrators who know one Security Fabric product need minimal training to manage them all
- All receive consistent OS updates, enabling consistent life cycle and policy management
- All log events in the same way, facilitating communication and data compilation for reporting and analysis
- All can leverage SOAR capabilities to improve threat response and reduce risk
- Are able to coordinate to address multipronged attacks across the organization's attack surface
- Are capable of receiving real-time, artificial intelligence (AI)-generated threat intelligence from FortiGuard Labs

Developing and maintaining a single network operating system translates into more strategic development of the Fortinet Security Fabric. This is because each component is developed with a consideration of its impact on the others. Customers can invest in the Security Fabric, confident that future developments will enhance the value of that investment.

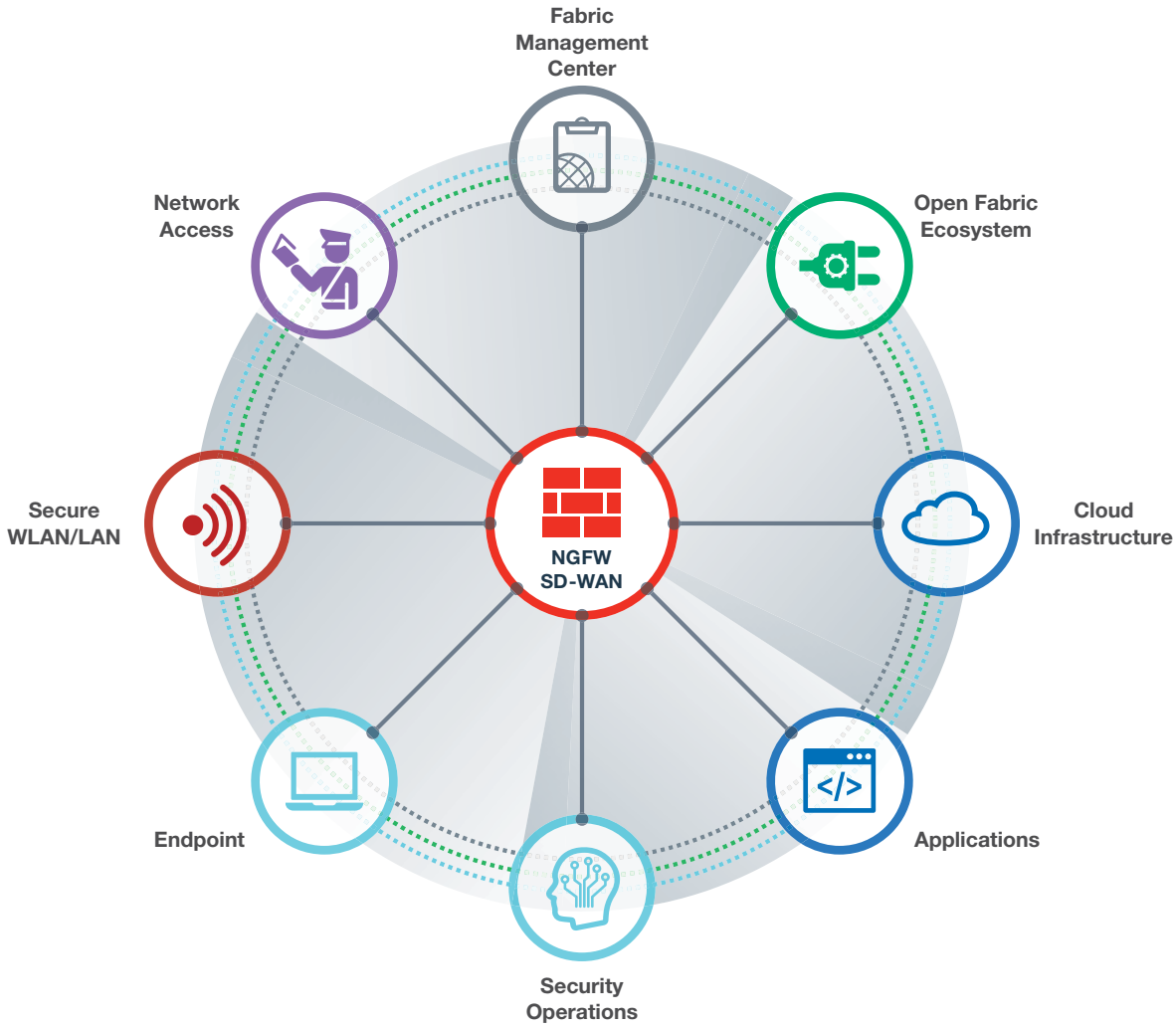

Figure 1: The Fortinet Security Fabric, built on the FortiOS network operating system, enables multiple security technologies to work seamlessly together, across all environments and supported by a single source of threat intelligence. This eliminates security gaps in the network and hastens responses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

Key Security Solution Areas Addressed

FortiOS 6.4 addresses the five pillars of the Security Fabric:

1. **Security-driven networking.** FortiGate NGFWs with secure web gateways (SWGs) manage security risks and block threats, and Fortinet Secure SD-WAN (software-defined wide-area network) improves and secures user and application experience.
2. **Zero-trust network access.** Zero-trust network access solutions, including FortiNAC and FortiAuthenticator, identify the devices and users on the network. The Fortinet Fabric Security Agent provides user and device tracking on and off the corporate network.
3. **Dynamic cloud security.** FortiGate NGFWs, FortiCASB cloud access security broker (CASB), and FortiCWP cloud workload protection (CWP) provide cloud security, access control, and configuration management. FortiWeb, FortiMail, and FortiCASB secure cloud-based web, email, and Software-as-a-Service (SaaS) applications.
4. **AI-based security operations.** AI-driven threat intelligence helps to predict and prevent attacks and detect unknown and insider threats. SOAR enables more rapid threat response and containment.
5. **Fabric Management Center.** Over 250 Fabric integrations enable centralized visibility and configuration management across an organization's security architecture. These also lay the foundation for automated security operations and report generation.

New Capabilities in FortiOS 6.4

As organizational networks evolve to meet DI goals, the Fortinet Security Fabric evolves to better secure them. The latest version of FortiOS includes many new features across all five solution areas. Together, they are designed to simplify the protection of growing attack surfaces from accelerating advanced threats. Following are some of the major enhancements:

Broader IoT device visibility

Deployment of IoT devices is a common component of DI initiatives, but these devices often have poor security by default, making them a threat to enterprise security. FortiOS 6.4 automatically detects IoT devices and assigns them to virtual LANs (VLANS). This supports integrated NAC, a crucial part of a zero-trust access strategy. This enables organizations to ensure that compromising one IoT device does not enable an intruder to move laterally throughout the network.

Integrated zero-trust network access

Zero-trust network access policies are further supported with the inclusion of authentication as an integral part of the Security Fabric management component. This means organizations no longer need to purchase a distinct solution to protect against the threats associated with compromised user credentials or malicious insiders within the Security Fabric.

FortiOS 6.4 Enables:

- Integrated access control
- Broader IoT device visibility
- Enhanced endpoint protection
- SIEM/SOAR integration in FortiAnalyzer

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.[4]

Automation, artificial intelligence, and machine learning are only being taken up by 38% of organizations.[5]

Enhanced endpoint protection

Enforcing security policies for devices connected to the on-premises corporate network is relatively straightforward, but organizations are increasingly reliant upon mobile devices for core business operations. The newest release of FortiOS 6.4 includes integration with FortiEDR endpoint detection and response (EDR). FortiEDR offers protection of devices on and off of the corporate network and enables lightweight protection of devices with extremely high availability requirements.

SIEM/SOAR integration in FortiAnalyzer

To address the growing problems of the cybersecurity skills gap and expanding organizational threat surface, additional automation capabilities are integrated into FortiAnalyzer with the latest FortiOS upgrade. Integrated SIEM and SOAR capabilities support more rapid, efficient, and automated incident detection and response. Organizations can now also define and link playbooks in FortiAnalyzer, enabling more structured and consistent responses to known and common threats.

Conclusion

As organizations embrace DI to operate more effectively and provide improved customer experiences, their networks and attack surfaces will continue to evolve. FortiOS version 6.2 clearly met the needs of its day, and the update to version 6.4 provides features designed to support organizations' current security needs. As organizational networks and attack surfaces expand and change, FortiOS will continue to evolve to meet their needs.

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

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

[3] "2019 State of the Cloud Report," Flexera, 2019.

[4] According to internal data from FortiGuard Labs.

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

FORTINET

www.fortinet.com

February 13, 2020 12:33 AM

593117-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\FortiOS\sb-FA-understanding-fortios-the-heart-of-the-fortinet-security-fabric-2132020-1233AM