SOLUTION BRIEF

FortiOS is the Foundation of the Fortinet Security Fabric

Executive Summary

The Fortinet Security Fabric is the industry's highest-performing and most expansive cybersecurity platform. And FortiOS, the Fortinet operating system, is the heart of the Fortinet Security Fabric. It ties all the Security Fabric's security and networking components together to ensure tight integration. This enables the convergence of networking and security functions to deliver a consistent security posture across the entire infrastructure, even highly dynamic environments, including hybrid deployments of hardware, software, and X-as-a-Service.

FortiOS 7.2 is packed with new features that enhance its ability to deliver coordinated real-time security across networks, endpoints, and clouds. It includes a powerful combination of:

- New inline security technologies for an online hybrid world
- New ways of consolidating security and networking across ZTNA, LAN Edge, and SD-WAN
- An industry-first unified networking and security architecture for OT, IoT, and IT devices
- New SOC and NOC process automation features for enhanced focus and seamless scale

FortiOS and the Fortinet Security Fabric Enable Broad, Integrated, and Automated Security

The Fortinet Security Fabric, built on FortiOS, enables multiple security and networking technologies to work together seamlessly across all environments, enhancing its ability to protect your organization through a single source of unified threat intelligence. This holistic approach eliminates security gaps in the network and hastens responses to attacks and breaches. And because FortiOS runs natively in any environment, it enables the Security Fabric to span and adapt to the extended digital attack surface for broad, integrated, and automated protection of devices, data, and applications wherever they are located.

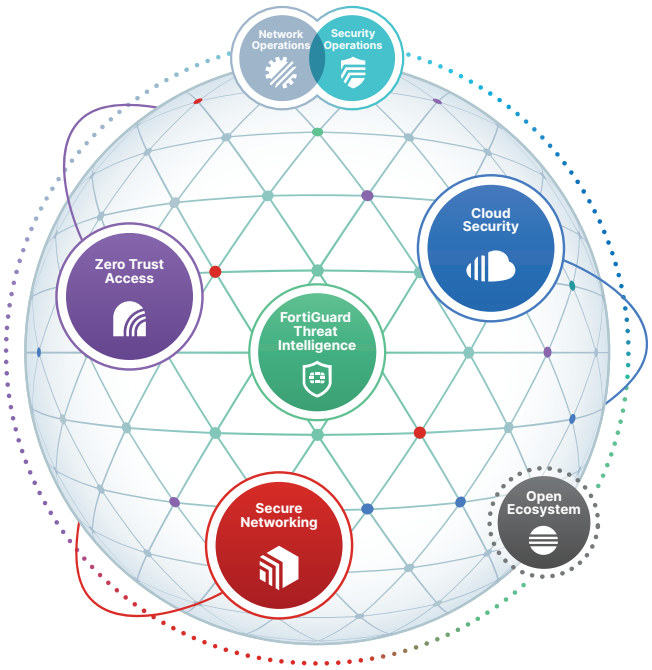

Figure 1: Fortinet Security Fabric diagram.

Having one unifying operating system that spans the entire distributed Security Fabric ensures:

- Consistent, centralized management and orchestration of security policy and configurations
- Broad reach and control across the expanded attack surface and at every step of the attack cycle
- High-performance enforcement of context-aware security policy
- Artificial intelligence (AI)-based threat detection and recommendations
- AI-based data correlation for analysis and reporting across a unified Fabric-level dataset
- Automated, multipronged response to cyberattacks across the attack surface and throughout the attack cycle
- Improved threat response and reduced risk through enhanced security orchestration, automation, and response (SOAR) capabilities

FortiOS 7.2 Delivers New Capabilities

FortiOS 7.2 addresses and elevates the complex challenges disrupting today's digital acceleration efforts. These include:

- Ineffective security intelligence with no real-time impact makes it impossible to keep ahead of never-seen-before automated attacks.
- Inability to coordinate security across an ever-expanding attack surface and evolving attack cycles creates exploitable security gaps.
- Silos between networking and security create operational and security deficiencies and heighten risk. This is especially challenging as IT and OT networks continue to converge.
- Distributed security postures make effective and consistent detection, prevention, and response in real time nearly impossible.

With over 300 new features spanning the entire Fortinet portfolio, FortiOS 7.2 uniquely empowers organizations to run their businesses without compromising performance, protection, or putting the brakes on innovation. It enables you to establish a consistent and dynamic security posture so users and devices can securely access applications and services from any location regardless of where they are deployed. It also continuously assesses risk and automatically adjusts enforcement end-to-end for any interaction from anywhere. And to expand our portfolio, this release also introduces several new NGFW models that enhance critical performance across today's hybrid networks.

Here are a few of the key FortiOS 7.2 enhancements designed to address today's unique challenges:

Inline Sandbox

FortiGuard Inline Sandbox Security Service plays a crucial role in stopping ransomware and other threats before damaging the organization. A FortiGate device detects and halts the delivery of a file while the sandbox quickly examines it. Only clean files are released to the user without introducing delays.

Next-Generation Firewall

Unified policy: Unified firewall policy configuration ensures all policies are managed and orchestrated through a single console, including ZTNA.

ZTNA service portal improvements: FortiGate now dynamically publishes its application list to FortiClient, bypassing the need for a second configuration on FortiClient EMS.

IPS admin enhancements: Role-based access control monitors and controls the release of signatures.

Global SOC-as-a-Service: This service provides log location and 24×7 SOC analysts along with managed firewall and endpoint triage.

Secure SD-WAN

Automated overlay orchestration: Simplifies and accelerates overlay orchestration on a global scale with best practices configurations built-in.

Large-scale zero-touch provisioning: Get device blueprints in minutes and easily apply device templates to sites at any scale.

Enhanced application and visibility: Enable per-application performance monitoring and MOS (mean opinion score) scoring for VoIP apps.

End-to-end segmentation: Segments and preserves LAN VRF (virtual routing and forwarding) traffic across a single overlay WAN segmentation.

Fabric self-orchestration: Allow devices inside the Fortinet Security Fabric to automatically build a secure overlay network for inter-site communication.

Traffic steering: FortiGuard categories can be used as destinations in SD-WAN rules to easily direct traffic based on business intent instead of specific rules or applications.

LAN EDGE

FortiSwitch: New enhancements further enhance network deployment with minimal technical expertise.

FortiLink NAC: Delivers improved visibility and segmentation, enabling the auto-discovery of devices to implement “least privilege” access.

Zero Trust Network Access (ZTNA)

SaaS application control: FortiOS 7.2 provides enhanced operational efficiencies and support for SaaS application control.

Operational Technology

Asset Identity Center: New dashboards show the network topology using the Purdue model, helping administrators better understand risk in the OT network. Provides insights into how risk in your industrial control system varies across different PLCs, HMIs, and other critical assets.

Air-gap license activation: This latest release simplifies and streamlines licensing in isolated environments.

OT detection and protection service (virtual patching): Enables compensating risk management control when patching is not an option.

FortiOS and the Fortinet Security Fabric Address Current and Emerging Security Challenges

The outcome of embracing digital transformation to operate more effectively and provide improved customer and worker experiences is largely determined by how well organizations apply effective security at every step. FortiOS 7.2 provides features to support today’s fast-changing hybrid networking and security needs.

FortiOS is continually updated to ensure organizations stay ahead of today’s ever-evolving threat landscape. With an expansive Fortinet Security Fabric solution in place, organizations of any size can be assured that they have the tools they need to address all their security and networking challenges, no matter how broadly their users and networks are distributed, today and into the future.

April 1, 2022 1:29 PM

1544164-0-0-EN