SOLUTION BRIEF

FortiOS Is the Foundation of the Fortinet Security Fabric

Executive Summary

FortiOS, Fortinet's operating system, is the foundation of the Fortinet Security Fabric. The Security Fabric is the industry's highest-performing and most expansive cybersecurity platform, organically built on a common management and security framework. FortiOS ties all of the Fabric's security and networking components together to ensure seamless integration. This enables the convergence of networking and security functions to deliver a consistent user experience and resilient security posture across all manner of environments. On-premises, cloud, hybrid, and converging IT/OT/IoT infrastructure are included.

"FortiOS … improves operational efficiency and provides consistent security no matter where users or applications are distributed."[1]

FortiOS 7.4 is packed with powerful new features that give IT leaders unprecedented visibility and enforcement across even the most complex hybrid environments. Updates include:

- Industry-first unified networking and security architecture for OT, IoT, and IT devices
- Industry-first unified management and analytics capabilities across Fortinet's entire secure networking portfolio through FortiAnalyzer
- Greater automation and real-time response capabilities for SOC teams to protect against and reduce time to resolution for sophisticated attacks such as weaponized AI attacks, targeted ransomware, and criminal-sponsored APTs
- Enhancements to reduce alert triage and incident investigation across early detection solutions including FortiEDR, FortiXDR, FortiRecon, and FortiDeceptor
- New features to reduce risk across converging OT/IT/IoT environments

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

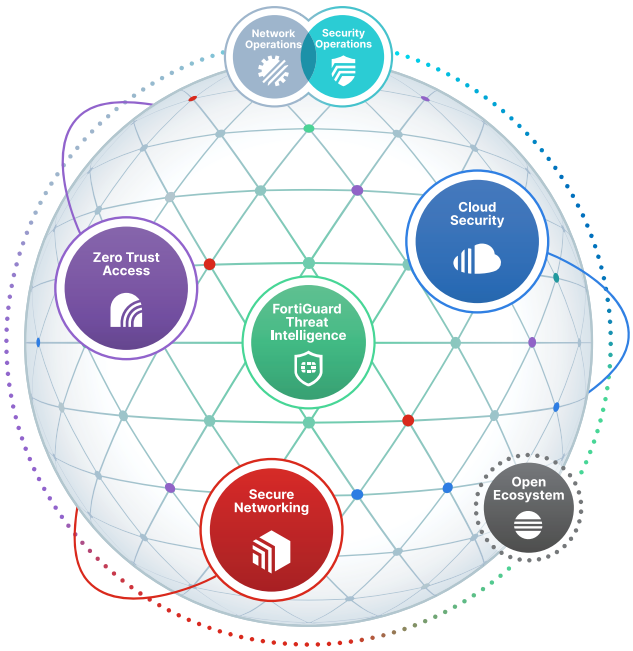

Figure 1: The Fortinet Security Fabric

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 in real time 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 7.4 Delivers New Capabilities

FortiOS uniquely empowers organizations to run their businesses without compromising performance, protection, or putting the brakes on innovation. A few of the key FortiOS 7.4 and Security Fabric enhancements designed to address today's unique challenges are listed below.

Secure networking and management

New innovations to Fortinet's Secure Networking Portfolio and FortiOS 7.4 span FortiManager, hybrid mesh firewall, Secure SD-WAN, single-vendor SASE, Universal zero-trust network access (ZTNA), and secure WLAN/LAN.

Unified management and analytics across hybrid networks

FortiManager provides IT leaders with unprecedented visibility and enforcement across all secure networking elements, including hybrid mesh firewall, single-vendor SASE, Universal ZTNA, Secure SD-WAN, and secure WLAN/LAN.

Hybrid mesh firewall for data center and cloud

FortiGate 7080F is a new series of next-generation firewalls (NGFWs) that eliminates point products, reduces complexity, and delivers higher performance through purpose-built ASIC technology and AI/ML-powered advanced security.

FortiFlex is a points-based consumption program with support for hybrid mesh firewall deployments and a variety of products, such as virtual machines, FortiGate appliances, and SaaS-based services, among others.

Secure SD-WAN for branch offices

Fortinet Secure SD-WAN enables consistent security and superior user experience for business-critical applications, whether in the cloud or on-premises, and supports a seamless transition to single-vendor SASE. New enhancements include automation in overlay orchestration to accelerate site deployments and a redesign of the monitoring map view to provide global WAN status for each.

Single-vendor SASE for remote users and branch offices

FortiSASE converges cloud-delivered security and networking to simplify operations across hybrid networks. FortiSASE now integrates with FortiManager, allowing unified policy management for Secure SD-WAN and SASE along with unmatched visibility across on-premises and remote users.

Universal ZTNA for remote users and campus locations

Fortinet Universal ZTNA provides the industry's most flexible zero-trust application access control no matter where the user or application is located. Universal ZTNA now delivers user-based risk scoring as part of our continuous checks for ongoing application access.

WLAN/LAN for branch offices and campus locations

FortiAP secure WLAN access points now integrate with FortiSASE, marking the industry's first AP integration with SASE. This enables secure micro-branches where an AP is deployed to send traffic to a FortiSASE solution and ensure comprehensive security of all devices at the site.

Prevention, early detection, and real-time response

Fortinet has added new real-time response and automation capabilities across the Security Fabric to enable SOC teams to protect against and reduce time to resolution for sophisticated attacks such as weaponized AI attacks, targeted ransomware, and criminal-sponsored APTs. New solutions and enhancements across five key areas include:

Endpoint security and early response

FortiEDR and **FortiXDR** now provide additional interactive incident visualization with enriched contextual incident data using multiple threat intelligence feeds to enable customers to simplify and expedite investigations.

"Via the power of the FortiOS operating system, FortiGate delivers one of the top secure SD-WAN solutions, includes a powerful LAN edge controller, enables the industry's only Universal ZTNA application gateway, and facilitates the convergence of NOC and SOC."[2]

FortiNDR Cloud combines robust artificial intelligence, complemented by pragmatic analysis and breach protection technology. The solution provides 365-day retention and visibility into network data, built-in playbooks, and threat hunting capabilities to detect anomalous and malicious behavior on the network. Choose from a self-contained, on-premises deployment powered by the Fortinet Virtual Security Analyst, or a new guided SaaS offering maintained by advanced threat experts from FortiGuard Labs.

FortiRecon, supported by threat experts from FortiGuard Labs, now delivers enhanced proactive threat intelligence into critical risks associated with supply chain vendors and partners, including external exposed assets, leaked data, and ransomware attack intelligence.

FortiDeceptor now offers vulnerability outbreak defense. When a vulnerability is reported by FortiGuard Labs, it is automatically pushed as a feed to the outbreak decoy to redirect attackers to fake assets and quarantine the attack early in the kill chain. Further, a SOAR playbook can automatically initiate the creation of and strategically place deception assets to gather granular intel and stop suspicious activities. FortiDeceptor also now offers a new attack exchange program that allows FortiDeceptor users to anonymously exchange valuable intel on the most current attacks and take proactive steps to avoid a breach.

SOC automation and augmentation

FortiAnalyzer enables more sophisticated event correlation across different types of log sources using a new intuitive rules editor that can be mapped to MITRE ATT&CK use cases.

FortiSOAR now offers a turnkey SaaS subscription option, inline playbook recommendations driven by machine learning, extensive OT security features and playbooks, and unique no/low-code playbook creation enhancements.

FortiSIEM now includes new link graph technology that allows for easy visualization of relationships between users, devices, and incidents. The solution is also now powered by an advanced machine learning framework, which enhances protection by detecting anomalies and outliers that may be missed by traditional methods.

FortiGuard SOC-as-a-Service now offers AI-assisted incident triage as well as new SOC operations readiness and compromise assessment services from FortiGuard Labs.

AI-powered threat intelligence

FortiGuard Industrial Security Service significantly reduces time to protection with enhanced automated virtual patching for both OT and IT devices based on global threat intelligence, zero-day research, and Common Vulnerabilities and Exposures (CVE) query service.

FortiGuard IoT Service enhances granular OT security at the industry level with Industrial-Internet-of-Things (IIoT) and Internet-of-Medical-Things (IoMT) device convergence.

FortiSIEM unified security analytics dashboards now incorporate mapping of industrial devices and communication paths to the Purdue model hierarchy, include new OT-specific playbooks for threat remediation, and use of the ICS MITRE ATT&CK matrix for OT threat analysis.

Identity and access

FortiPAM privileged account management provides remote access for IT and OT networks. It now includes ZTNA controls when users try to access critical assets. The ZTNA tags can be applied to check device posture continuously for vulnerabilities, updated AV signatures, location, and machine groups.

Application security

FortiDevSec provides comprehensive application security testing for application code and runtime applications. The solution incorporates SAST, DAST, and SCA, for early vulnerability and misconfigurations detection, and protection including secret discovery.

Risk reduction for cyber-physical and industrial control systems

Fortinet's portfolio of solutions and our Security Fabric for OT are designed specifically for cyber-physical security. New enhancements include:

FortiGate 70F Rugged Next-Generation Firewall (NGFW) is the latest addition to Fortinet's rugged portfolio designed for harsh environments. It features a new compact design with converged networking and security capabilities on a single processor.

FortiDeceptor Rugged 100G is now available as an industrially hardened rugged appliance, ideal for harsh industrial environments.

FortiPAM offers enterprise-grade privileged access management for both IT and OT ecosystems.

FortiSIEM unified security analytics dashboards now include event correlation and mapping of security events to the Purdue model.

FortiSOAR now offers features to reduce alert fatigue and enable security automation and orchestration across IT and OT environments.

FortiGuard Industrial Security Service now includes more than 2,000 application control signatures for OT applications and protocols that support deep packet inspection.

Fortinet Cyber Threat Assessment Program (CTAP) for OT validates OT network security effectiveness, application flows, and includes expert guidance.

OT tabletop exercises for OT security teams are led by FortiGuard Incident Response team facilitators with expertise in threat analysis, mitigation, and incident response.

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

FortiOS 7.4 provides features and enhancements 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 in the future.

[1] "Ken Xie Q&A: Growth, Differentiators, and FortiSP5," Fortinet, February 13, 2023.

[2] John Maddison, "Setting the Record Straight on Competitor Misinformation," Fortinet, November 11, 2022.

April 13, 2023 8:15 AM
1544164-A-0-EN