WHITE PAPER

Introducing FortiOS 7.6

Enhancing Fortinet's Real-Time Network Security Operating System

The Need for Integrated Security

For decades, the cybersecurity landscape has been dominated by a siloed approach, with isolated products deployed across the network and networking and security existing as separate entities. This fragmented strategy leaves significant vulnerabilities, forcing organizations to cobble together disparate point solutions that create complexity and hinder visibility. Fortinet, however, has always championed a different vision: the convergence of networking and security. Founded on the principle of integrated security, we recognize that true network protection requires a holistic platform approach.

Our longstanding commitment to developing and delivering a unified platform is further solidified with the release of FortiOS 7.6, the latest update to our industry-leading operating system. This update injects new capabilities and services across the Fortinet Security Fabric, the most mature and comprehensive cybersecurity platform in the market today. Unlike competitors just now jumping on the platform bandwagon, we have been diligently building and refining the Security Fabric for years, resulting in the most extensive product coverage available. These latest enhancements to the Security Fabric include adding new generative AI capabilities across all three of our pillars, adding new managed services for our firewall, SASE, and SOC operations, new integrations for our Unified agent, and new data protection.

"FortiOS is the world's most powerful, real-time network security operating system capable of simplifying management across content, applications, users, devices, data, and locations."

Ken Xie
Fortinet Founder,
Chairman of the Board,
and Chief Executive Office

The power of this unified platform approach lies in its singular core:

- **One Operating System (FortiOS):** Our commitment to delivering an integrated network and security platform built on a single OS is evident in our industry-leading position across multiple Gartner Magic Quadrant categories, including Firewalls, LAN Edge, SD-WAN, and Secure Access Service Edge (SASE)—all powered by the same FortiOS. This integrated approach eliminates the complexity of managing disparate systems and ensures consistent security policies and enforcement across your entire network.
- **One Unified Agent (FortiClient):** The Fortinet agent provides unmatched telemetry, visibility, and control to IT teams. It seamlessly integrates Endpoint Protection Platform (EPP) and Zero Trust Network Access (ZTNA) capabilities, and with the coming addition of Endpoint Detection and Response (EDR), offers a comprehensive security posture for your endpoints that can also be seamlessly integrated with the rest of your network security framework and SOC environment.
- **One Management Tool (FortiManager):** Our unified management tool delivers centralized control across your entire hybrid environment, from your campus and data centers to your branch offices and remote users to your multi-cloud environments. FortiManager simplifies the management of on-premises, cloud-based, and cloud-delivered security solutions, offering a single pane of glass for comprehensive network visibility and control.
- **One Data Lake (FortiAnalyzer):** Our newly announced data lake serves as a central repository for Security Operations Center (SOC) analysis. This unified data platform streamlines threat detection, investigation, and response, empowering your security team to make faster and more informed decisions.

By leveraging a single OS, agent, management tool, and data lake, the Fortinet Security Fabric shatters the limitations of siloed security solutions. This inherent unity fosters exceptional integration, simplifies management, and empowers your security team with unparalleled visibility and control.

While others may use platforms to create vendor lock-in, we are committed to maintaining and expanding the industry's broadest, open ecosystem of partners. This approach ensures the Fortinet Security Fabric remains a multi-vendor platform solution that seamlessly integrates with your existing security infrastructure, protecting security investments and allowing flexibility when selecting security vendors.

Enhancements in FortiOS 7.6

The Fortinet Security Fabric platform is delivered across critical use cases, providing a broad range of integrated security and network functionality to every corner of the network. The latest enhancements in FOS 7.6 provide new or enriched capabilities in the following areas:

Secure Networking

The Secure Networking component of the Fortinet Security Fabric combines critical networking, connectivity, and security functions, including OT, IOT, and Edge security.

FOS 7.6 enhancements include:

- **FortiAI for Management, Provisioning, Docs, & Support:** Forti AI now includes Generative AI within FortiManager to assist with platform management, new product and feature deployment, network monitoring, and accessing documentation and support assets. FortiAI facilitates faster decision making, helps detect and remediate incidents quickly, and ensures organizations can easily adopt the technologies they require.
- **Managed FortiGate Service:** This new service can offload NOC teams by deploying, configuring, monitoring, and managing FortiGate deployments. Staffed by Fortinet professionals, this service leverages cloud-based tools to become an extension of the NOC team. Customers and partners can use these services so their cybersecurity experts can focus on higher-value activities.
- **Data Loss Prevention:** DLP enhancements improve detection confidence and exact match capabilities to ensure sensitive information remains secure no matter where it resides within the hybrid network.
- **FortiLink NAC:** Enhancements to our in-built NAC capability, part of our proprietary FortiLink protocol, enable FortiGate devices to directly manage FortiSwitch and FortiAP products. FortiLink NAC enables Fortinet switches and access points to identify and properly onboard IoT devices into the appropriate network segment without requiring additional licenses.
- **Wi-Fi 7 Controller:** Our wireless controller can now manage our recently announced Wi-Fi 7 access points.
- New AIOps services improve SD-WAN monitoring and management and DEM's ability to share information, resulting in better visibility and better user experiences.
- **New FortiGuard Services:** FortiGuard Services provides organizations with a proactive and intelligent approach to cybersecurity, enabling them to confidently navigate the ever-changing threat landscape. Enhancements to our existing suite of AI-powered services include:
  - **Increased FortiGate NGFW inline protection capabilities:** Real-time inline detection and prevention of AI-powered attacks can recognize and block even the most intricate and novel threats
    - Significant upgrades to the AI-powered Inline Malware Prevention Service include new features like real-time anti-phishing and an accelerated AI pre-filter
    - The ability to render verdicts more quickly
    - Critical prevention of patient zeros
    - AI enhancements to URL and web filtering to improve malicious attack prevention

Unified SASE

As organizations incorporate more cloud-based resources and support a hybrid workforce, cloud-delivered and cloud-based security solutions grow in importance. Securing remote users while maintaining reliable connections is paramount for organizations that have adopted a hybrid workforce strategy. FortiOS 7.6 enhancements include:

- **Unified Agent (FortiClient):** FortiClient converges many solutions into a single agent, including ZTNA, VPN, EPP, continuous vulnerability assessment, sandboxing, telemetry, and DEM, as well as agent capabilities for PAM and NAC. FortiOS 7.6 adds a complete EDR capability to FortiClient, adding ransomware protection, behavior-based detections, and automated responses to its host of visibility, control, and remote access capabilities.
- **SASE (SSE + SD-WAN):**
  - **Managed SASE/ZTNA:** Similar to the Managed FortiClient service, the FortiSASE operations team can onboard a SASE customer and help configure their SASE portal. This remote service and its managed service engineers will configure FortiSASE, offloading local NOC or SOC teams from managing this element of their cybersecurtiy.
  - **FortiAI for migration, planning, and deployment:** New Generative AI can assist with transitioning to public clouds and provide guidance on planning and deploying applications and services within specific cloud platforms. This service will be available within cloud provider offerings, such as FortiAI for AWS and FortiAI for Azure.
  - **Data protection:** DLP enhancements improve detection confidence levels and its exact match capabilities for SASE users to ensure sensitive information remains secure no matter where it resides within the hybrid network.
  - **Switch/AP/5G Support:** New FortiSASE support for thin edge use cases enables remote AP, switch, and FortiExtender deployments.
  - **SD-WAN:** FortiOS 7.6 provides over 20 new SD-WAN capabilities to streamline operations and improve user experience. Enhancements to Overlay Orchestration simplify and automate connectivity across multiple clouds to streamline operations. Improvements to our Underlay Bandwidth and Quality Monitoring Service offer comprehensive link, path, and application performance monitoring to optimize user experience and simplify operations.
  - **Remote Browser Isolation:** Organizations can now easily add RBI (remote browser isolation) to their SASE user set to further insulate users from the threats on the internet.
  - **End-to-End Digital Experience Monitoring (DEM):** The DEM agent has now been added to FortiClient, offering end-to-end DEM for FortiSASE users for better visibility and troubleshooting.
  - **3rd Party SSE Support (IPSec):** FortiSASE IPsec Service Connection allows prospects to connect third-party SD-WAN branches and regular routers to the FortiSASE platform using IPSec tunnels. This enables greater flexibility when selecting and managing vendors and vendor transitions.
  - **Unified Policy:** Leveraging the common FortiOS deployed across on-prem and virtual firewalls and SASE POPs, users can establish unified policies across all their firewall enforcement points.

AI-Powered SOC Operations

Detecting, preventing, and remediating threats and attacks continue to be critical challenges for many SOC teams. That's why we have developed advanced AI capabilities for SOC environments that enhance threat identification, including generative AI to guide SOC teams in threat investigation and response.

FortiAnalyzer 7.6, the central data lake of the Fortinet Security Fabric, unifies configurations, events, and alerts and provides advanced threat visualization views. It also introduces a Security Automation Subscription that offers powerful features like premium reports, event handlers, and incident response playbooks. These enhancements empower SecOps teams and streamline operations with improved detection, investigation, and response to security incidents. New FortiOS 7.6 enhancements include:

- **Enhanced SOC-as-a-Service (SOCaaS):** Integrating SOCaaS with SASE, Forensics, and MFGS, along with integrating outbreak detection capabilities, significantly enhances our managed SOC offering.
- **FortiAI Integration:** Integrating FortiAI into FortiAnalyzer enhances the system's ability to analyze and respond to security threats. By leveraging FortiOS telemetry data, FortiAI provides advisory support, facilitating quicker decision-making and efficient actions like specific report queries or event handling.

- **SIEM Lite:** Adding limited SIEM capabilities to FortiAnalyzer helps centralize data in the Security Fabric by merging configurations, events, and alerts for better visibility and analysis. Its threat visualization dashboards (including interactive topology) offer an intuitive, graphical representation of security threats and patterns.
- **SOAR Lite:** Adding limited SOAR capability to FortiAnalyzer, accessible through the Security Automation Subscription, offers curated content packs with out-of-the-box premium reports, event handlers, advanced correlation rules, third-party log parsers, automation connectors, data enrichment, and incident response playbooks. These packs provide a significant advantage as they will be updated continuously, independent of future FortiAnalyzer releases, ensuring that SecOps teams have the most current tools and data at their fingertips.
- **Governance, Risk, and Compliance (GRC):** FortiAnalyzer 7.6 addresses the complexities of adhering to, maintaining, and continuously improving compliance and risk management while catering to the dynamic nature of security infrastructures with new GRC reports. Its service for attack surface and compliance management proactively assesses network vulnerabilities and helps guide targeted improvements in security posture. These tools simplify the compliance process by automatically generating reports on industry-specific risks and non-compliant configurations, offering valuable insights into the security posture of IT and OT environments.
- **FortiAI for Incident Response:** Generative AI assistance can analyze alerts and alarms in FortiSIEM and provide prompts for follow-up actions in FortiSIEM and FortiSOAR.
- **EDR integration with FortiClient:** Adding EDR to FortiClient brings full endpoint detection and response capabilities to our Unified Agent, including combining ransomware protection and ZTNA capabilities in one agent.

The Fortinet Advantage

Fortinet provides the industry's most complete and robust cybersecurity platform. Since our founding over twenty years ago, we have been focused on organic innovation and product development, complemented by tactical acquisitions for specific technologies or capabilities, to create the industry's most holistic and integrated cybersecurity and networking solution strategy.

This relentless pursuit of an integrated Security Fabric has enabled us to deliver a platform built around one operating system, one unified agent, one management console, and one data lake. Studies have shown how this platform approach produces better security outcomes, more efficient operations, a better user experience, and a stronger ROI.

FortiOS 7.6 builds on our previous extensive development, with the latest in generative AI, managed services, and advanced functionality to further speed and simplify today's increasingly complex NOC and SOC operations.

March 29, 2024 1:19 PM

2641038-0-0-EN