



FortiOS 6.4

Effective AI-Driven Security Operations

In the reality of today's market, digital innovation—across on-premises, cloud, and applications to users and devices—is critical. However, complexities and blind spots abound.

Attackers understand this all too well and aim to exploit those blind spots to carry out successful attacks and compromises. Worse yet, based on research conducted by FortiGuard Labs, we believe that the future of cyberattacks will be heavily influenced by swarmbots—where cyber criminals leverage machine learning/artificial intelligence (ML/AI) to attack networks and devices in a coordinated and simultaneous fashion.

In addition to the accelerating pace of cyberattacks, the growth of unsecure or unknown devices attaching to the network, along with a host of breaches resulting from stolen credentials, often stretches security teams to a breaking point.

For organizations to achieve their digital innovation outcomes while effectively managing complexity and defending against advanced threats, teams need a broad, integrated, and automated cybersecurity platform such as the Fortinet Security Fabric.

FortiOS, a security-hardened, purpose-built network operating system, is the software foundation of the entire Fortinet Security Fabric. Designed to deliver tightly integrated and intuitive security and networking capabilities across the entire organization, FortiOS delivers everything from core network functionality to best-in-class security that protects organizations end to end, including the ability to extend the Fortinet Security Fabric to third-party solutions using application programming interfaces (APIs) and Security Fabric connectors. FortiOS also provides seamless automation and orchestration, helping organizations overcome resource challenges and skills gaps.

The FortiOS 6.4 logo icon, which consists of a shield with three horizontal lines inside, enclosed in a circular border, with the number 6.4 below it.

FortiOS provides seamless automation and orchestration, helping organizations overcome resource challenges and skills gaps.

With this latest release of FortiOS, and its integrated components, Fortinet customers can expect to detect more (and more sophisticated) threats as well as respond to and remediate issues faster—regardless of their level of security operations center (SOC) maturity.

FortiOS 6.4 and the Fortinet Security Fabric now include new, ML-based advanced threat-protection capabilities at the endpoint (FortiEDR) and across network, web application, and email attack vectors (FortiSandbox and FortiAI). At the same time, it increases SOC visibility, automation, and orchestration with FortiAnalyzer, FortiSIEM, and FortiSOAR, each of which helps response across the native Fortinet Security Fabric, across third-party solutions deployed throughout the environment, and across a multifunction SOC.

Automation Across the Security Fabric

The centralized, single-pane visibility of FortiOS 6.4 (FortiAnalyzer) delivers new high-value, baseline security orchestration, automation, and response (SOAR) capabilities across the Fortinet components of the Security Fabric. “Lite” playbooks guide response and increase operational efficiency.

Deeper Multivendor Views

In most large organizations, particularly those undergoing digital innovation, there are usually multiple solutions, technologies, and vendors. The Fortinet Security Fabric offers a large ecosystem of Fabric connectors and APIs to integrate and help manage this diverse environment in unison. In addition, FortiSIEM pulls in deeper data and visibility across Fortinet and third-party IT and security components.

New ML and advanced analytics detect lateral movement. Multivendor incident views, along with case management, aid in rapid investigation and coordinated response across teams and products.

New SOC Orchestration

For organizations with a mature SOC, where security operations processes are well-defined, FortiOS 6.4 and the Security Fabric include new advanced SOAR capabilities. These include correlated alerts into unified incidents, ML-based prioritization and assignment, automated enrichment, robust visual playbook-guided response, and more, all from the new FortiSOAR. Saving time, especially during breaches, is essential for complex, larger, and/or critical environments, organizations with stringent compliance reporting requirements, and companies with high-value intellectual property—for example, customers in the financial, healthcare, or defense industries.



The Fortinet Security Fabric offers a large ecosystem of Fabric connectors and APIs to integrate and help manage this diverse environment in unison.



FortiOS 6.4 and the Security Fabric include new advanced SOAR capabilities.

Services and Subscriptions

FortiOS 6.4 delivers several new and enhanced services and subscriptions for the Fortinet Security Fabric to help customers better operate and secure their networks. This includes a new Internet-of-Things (IoT) service that works with FortiOS 6.4 capabilities to shrink the IoT attack surface by automatically identifying, segmenting, and enforcing policies against IoT devices. FortiOS 6.4 also introduces enhancements to the Fortinet Security Rating subscription service.

The Fortinet Security Rating subscription service helps organizations achieve compliance and fix deficiencies and risks by providing visibility and checks against compliance and best-practice standards. This service also allows for benchmarking against other industry-peer organizations. FortiOS 6.4 enhances the Security Rating capability with an operations-centric view to help networking staff better prioritize and manage their environments.

The new and enhanced services are available as part of FortiGuard Enterprise and 360 Protection bundles, and as a la carte subscriptions that customers can use to customize their services.

Digital innovation requires a broad, integrated, and automated cybersecurity platform that only the Fortinet Security Fabric can provide. FortiOS 6.4 advances the Fortinet Security Fabric with greater security while delivering even more simplicity and automation to help customers better deploy, operate, and maintain network and security operations throughout their organization. For the SOC, this translates to qualitative reduction in complexity, time to detect and respond, resource burden, and skills gap.



The Fortinet Security Rating subscription service helps organizations achieve compliance and correct deficiencies and risks by providing visibility and checks against compliance and best-practice standards.