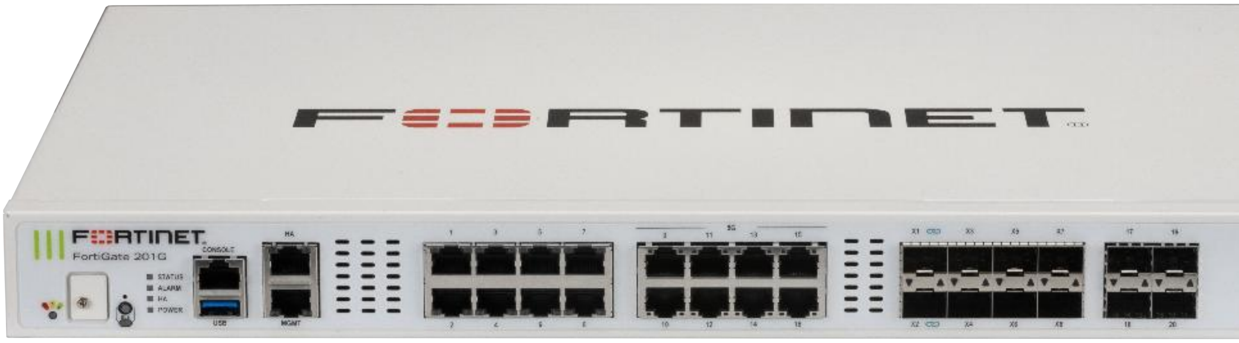
FORTINET

Data Sheet

# FortiGate 200G Series

Digitally signed by Cioban Alexei
Date: 2025.09.13 22:18:42 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ



## Highlights

**Gartner® Magic Quadrant™ Leaders** for both Network Firewalls and WAN Edge Infrastructure

**Secure Networking** with FortiOS for converged networking and security

**State-of-the-art unparalleled performance** with Fortinet's patented SPU and vSPU processors

**Enterprise security** with consolidated AI/ ML-powered FortiGuard services

**Deep visibility** into applications, users, and devices beyond traditional firewall techniques

## Artificial Intelligence, Machine Learning Security with Deep Visibility

The FortiGate 200G series next-generation firewall (NGFW) combines artificial intelligence (AI)-powered security and machine learning (ML) to deliver threat protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 200G Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks. This security fabric seamlessly extends across your entire environment, including a Hybrid Mesh Firewall architecture, ensuring consistent policy enforcement and threat protection across all network segments.

Universal zero-trust network access (ZTNA) automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast threat protection and SSL inspection provides security at the edge you can see without impacting performance.

| IPS | NGFW | Threat Protection | Interfaces |
|---|---|---|---|
| 9 Gbps | 7 Gbps | 6 Gbps | Multiple GE RJ45, 5GE RJ45, 10GE SFP+ Slots, GE SFP Slots |

## Use Cases

### Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-Powered Security Services, natively integrated with your NGFW, secures web, content, and devices and protects networks from ransomware, malware, zero days, and sophisticated AI-powered cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU technology provides industry-leading high-performance protection

### Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for hybrid working models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

### Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

### Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security from the branch to the data center and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services, detects and prevents known, zero-day, and unknown attacks

## FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

### Network and file security

Network and file security services protect against network and file-based threats. With over 18,000 signatures, our industry-leading intrusion prevention system (IPS) uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, and applying virtual patches for newly discovered vulnerabilities. Anti-malware protection defends against both known and unknown file-based threats, combining antivirus and sandboxing for multi-layered security. Application control improves security compliance and provides real-time visibility into applications and usage.

### Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of over 300 million URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks. FortiGuard Labs blocks over 500 million malicious/phishing/ spam URLs weekly, and blocks 32,000 botnet command-and-control attempts every minute, demonstrating the robust protection offered through Fortinet.

### SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This includes data loss prevention to ensure visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. Our inline cloud access security broker service protects data in motion, at rest, and in the cloud, enforcing compliance standards and managing account, user, and cloud app usage. Services also assess infrastructure, validate configurations, and highlight risks and vulnerabilities, including IoT device detection and vulnerability correlation.

### Zero-Day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown malware in real time, delivering sub-second protection across all NGFWs. The service also integrates the MITRE ATT&CK matrix to speed up investigations. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

### OT security

With over 1000 virtual patches, 1100+ OT applications, and 3300+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.

Available in

Appliance

Virtual

Hosted

Cloud

Container

# FortiOS Everywhere

### FortiOS, Fortinet's Real-Time Network Security Operating System

FortiOS is the operating system that powers Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. FortiOS provides a unified framework for managing and securing networks, cloud-based, hybrid, or a convergence of IT, OT, and IoT. FortiOS enables seamless and efficient interoperation across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances overall security posture. Together, FortiGate and FortiOS create intelligent, adaptive protection to help organizations reduce complexity, eliminate security silos, and optimize user experience.

By integrating generative AI (GenAI), FortiOS further enhances the ability to analyze network traffic and threat intelligence, detects deviations or anomalies more effectively, and provides more precise remediation recommendations, ensuring minimum performance impact without compromising security.

Learn more about what's new in FortiOS. [https://www.fortinet.com/products/fortigate/fortios](https://www.fortinet.com/products/fortigate/fortios)

*Intuitive easy to use view into the network and endpoint vulnerabilities*

*Comprehensive view of network performance, security, and system status*

## Fortinet ASICs: Unrivaled Security, Unprecedented Performance

### Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

### Network processor NP7Lite

Fortinet's new, breakthrough SPU NP7Lite network processor works in line with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP, and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

### Content processor CP10

Content processors act as co-processors to offload resource-intensive processing of security functions. The tenth generation of the Fortinet Content Processor, the CP10, accelerates resource-intensive security functions while delivering:

- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload

## FortiManager

### Centralized management at scale for distributed enterprises

FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides real-time monitoring of the entire managed infrastructure and automates network operation workflows. Leveraging GenAI  in FortiAI, it further enhances Day 0–1 configurations and provisioning, and Day N troubleshooting and maintenance, unlocking the full potential of the Fortinet Security Fabric and significantly boosting operational efficiency.

*GenAI in FortiManager helps manage networks effortlessly—generates configuration and policy scripts, troubleshoots issues, and executes recommended actions.*

## FortiConverter Service

### Migration to FortiGate NGFW made easy

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

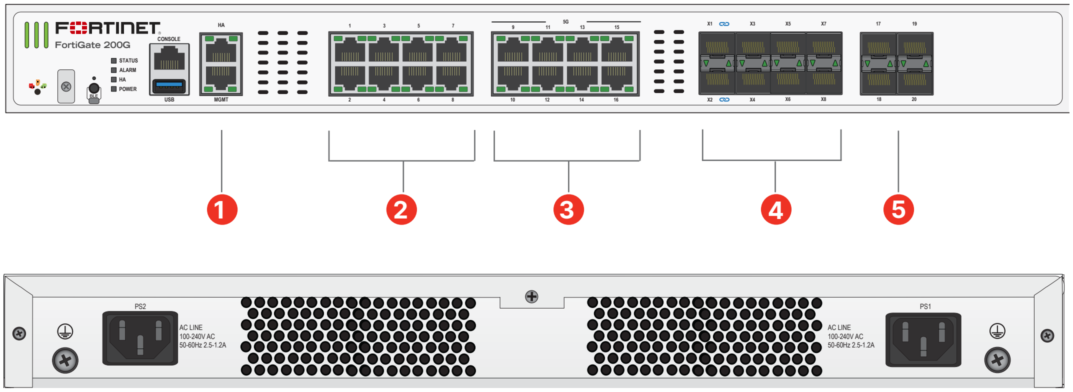
## FortiCare Services

### Expertise at your service

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

# Hardware

## FortiGate 200G Series



### Interfaces

1. 2 x GE RJ45 MGMT/HA Ports
2. 8 x GE RJ45 Ports
3. 8 × 5/2.5/GE RJ45 Ports
4. 8 × 10 GE SFP+/SFP FortiLink Slots
5. 4 x GE SFP Slots

### Hardware Features

■ NP7Lite (SP5) ■ CP10 ■ TPM ◣ 1RU ⚙ DUAL AC ● 10/5/GE ■ 480GB

### Trusted Platform Module (TPM)

The FortiGate 200G series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

### Dual power supply

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 200G series offers dual built-in non-hot swappable power supplies.

### Access layer security

FortiLink protocol enables you to converge security and network access by integrating the FortiSwitch into the FortiGate as a logical extension of the firewall. These FortiLink-enabled ports can be reconfigured as regular ports as needed.

### Signed Firmware Hardware Switch

The signed firmware switch is a physical security switch. It is by default set to the highest security level. The highest security level ensures that only an appropriately validated FortiOS firmware can be loaded on the FortiGate. This feature adds an additional physical layer of security to the FortiGate, acting as a key deterrent to and reducing risk of compromise.

# Specifications

| | FORTIGATE 200G | FORTIGATE 201G |
|---|---|---|
| **Interfaces and Modules** | | |
| **GE RJ45 Ports** | 8 | |
| **GE RJ45 Management / HA** | 1 / 1 | |
| **5/2.5/GE RJ45 Ports** | 8 | |
| **GE SFP Slots** | 4 | |
| **10/GE SFP/+ FortiLink Slots (default)** | 8 | |
| **USB Port** | 1 | |
| **Console Port** | 1 | |
| **Onboard Storage** | 0 | 1× 480 GB SSD |
| **Trusted Platform Module (TPM)** | ✓ | |
| **Bluetooth Low Energy (BLE)** | ✓ | |
| **Signed Firmware Hardware Switch** | ✓ | |
| **Included Transceivers** | 0 | |
| **System Performance — Enterprise Traffic Mix** | | |
| **IPS Throughput** [2] | 9 Gbps | |
| **NGFW Throughput** [2, 4] | 7 Gbps | |
| **Threat Protection Throughput** [2, 5] | 6 Gbps | |
| **System Performance and Capacity** | | |
| **IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)** | 39 / 39 / 26.5 Gbps | |
| **IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)** | 39 / 39 / 26.5 Gbps | |
| **Firewall Latency (64 byte, UDP)** | 4.36 μs | |
| **Firewall Throughput (Packet per Second)** | 39.75 Mpps | |
| **Concurrent Sessions (TCP)** | 11 Million | |
| **New Sessions/Second (TCP)** | 400 000 | |
| **Firewall Policies** | 10 000 | |
| **IPsec VPN Throughput (512 byte)** [1] | 36 Gbps | |
| **Gateway-to-Gateway IPsec VPN Tunnels** | 2000 | |
| **Client-to-Gateway IPsec VPN Tunnels** | 16 000 | |
| **SSL-VPN Throughput**[6] | 3 Gbps | |
| **Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)** | 500 | |
| **SSL Inspection Throughput (IPS, avg. HTTPS)** [3] | 7 Gbps | |
| **SSL Inspection CPS (IPS, avg. HTTPS)** [3] | 7100 | |
| **SSL Inspection Concurrent Session (IPS, avg. HTTPS)** [3] | 900 000 | |
| **Application Control Throughput (HTTP 64K)** [2] | 27.8 Gbps | |
| **CAPWAP Throughput (HTTP 64K)** | 37.5 Gbps | |
| **Virtual Domains (Default / Maximum)** | 10 / 25 | |
| **Maximum Number of FortiSwitches Supported** | 64 | |
| **Maximum Number of FortiAPs (Total / Tunnel)** | 256 / 128 | |
| **Maximum Number of FortiTokens** | 5000 | |
| **High Availability Configurations** | Active-Active, Active-Passive, Clustering | |

| | FORTIGATE 200G | FORTIGATE 201G |
|---|---|---|
| **Dimensions and Power** | | |
| **Height x Width x Length (inches)** | 1.75 × 17.0 × 15.0 | |
| **Height x Width x Length (mm)** | 44.45 × 432 × 380 | |
| **Weight** | 14.11 lbs (6.4 kg) | 14.33 lbs (6.5 kg) |
| **Form Factor (supports EIA/non-EIA standards)** | Rack Mount, 1 RU | |
| **AC Power Consumption (Average / Maximum)** | 145 W / 175 W | 145 W / 176 W |
| **AC Power Input** | 100–240V AC, 50/60Hz | |
| **AC Current (Maximum)** | 2A @100VAC, 1.2A @240VAC | |
| **Heat Dissipation** | 597.12 BTU/h | 600.54 BTU/h |
| **Power Supply Efficiency Rating** | 80Plus Compliant | |
| **Redundant Power Supplies** | ✓<br>(Default dual non-swappable AC PSU for 1+1 Redundancy) | |
| **Operating Environment and Certifications** | | |
| **Operating Temperature** | 32°F to 104°F (0°C to 40°C) | |
| **Storage Temperature** | -31°F to 158°F (-35°C to 70°C) | |
| **Humidity** | 5% to 90% non-condensing | |
| **Noise Level** | LPA 48 dBA / LWA 55 dBA | |
| **Forced Airflow** | Side and Front to Back | |
| **Operating Altitude** | Up to 10 000 ft (3048 m) | |
| **Compliance** | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB | |
| **Certification** | USGv6/IPv6 | |

Note: All performance values are "up to" and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

[6] Uses RSA-2048 certificate.

## Subscriptions

| | | | Bundles | | |
|---|---|---|---|---|---|
| **Service Category** | **Service Offering** | **A-la-carte** | **Enterprise Protection** | **Unified Threat Protection** | **Advanced Threat Protection** |
| **FortiGuard Security Services** | **IPS — IPS, Malicious/Botnet URLs** | • | • | • | • |
| | **Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [3], AI-based Heurestic AV, FortiGate Cloud Sandbox** | • | • | • | • |
| | **URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate** | • | • | • | |
| | **Anti-Spam** | | • | • | |
| | **AI-based Inline Malware Prevention [3]** | • | • | | |
| | **Data Loss Prevention (DLP) [1]** | • | • | | |
| | **Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check** | • | • | | |
| | **OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]** | • | | | |
| | **Application Control** | | ------------included with FortiCare Subscription----------- | | |
| | **Inline CASB [3]** | | ------------included with FortiCare Subscription----------- | | |
| **SD-WAN and SASE Services** | **SD-WAN Underlay Bandwidth and Quality Monitoring** | Models up to FG/ FWF-60F series | | | |
| | **SD-WAN Underlay and Application Monitoring Service** | FG-70F series and above | | | |
| | **SD-WAN Overlay-as-a-Service** | • | | | |
| | **SD-WAN Connector for FortiSASE Secure Private Access** | • | | | |
| | **SASE expansion for SD-WAN (SD-WAN SPA Connector license plus FortiSASE starter kit for n* users) [2]** | Selected models only[2] | | | |
| | **SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth)** | Desktop models only | | | |
| **NOC and SOC Services** | **FortiConverter Service for one time configuration conversion** | • | • | | |
| | **Managed FortiGate Service—available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management** | • | | | |
| | **FortiGate Cloud—Management, Analysis, and One Year Log Retention** | • | | | |
| | **FortiManager Cloud** | • | | | |
| | **FortiAnalyzer Cloud** | • | | | |
| | **FortiGuard SOCaaS—24×7 cloud-based managed log monitoring, incident triage, and SOC escalation service** | • | | | |
| **Hardware and Software Support** | **FortiCare Essentials** | Desktop models only | | | |
| | **FortiCare Premium** | • | • | • | • |
| | **FortiCare Elite** | • | | | |
| **Base Services** | **Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing** | | ------------included with FortiCare Subscription----------- | | |

1. Full features available when running FortiOS 7.4.1.

2. See the FortiSASE Ordering Guide for supported models and their associated number of user licenses.

3. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.

### FortiGuard Bundles

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

# Ordering Information

| Product | SKU | Description |
|---|---|---|
| **FortiGate 200G** | FG-200G | 10x GE RJ45 (including 1x MGMT port, 1x HA port, 8x switch ports), 4x GE SFP slots, 8× 5GE RJ45, 8× 10GE SFP+ slots, NP7Lite and CP10 hardware accelerated. |
| **FortiGate 201G** | FG-201G | 10x GE RJ45 (including 1x MGMT port, 1x HA port, 8x switch ports), 4x GE SFP slots, 8× 5GE RJ45, 8× 10GE SFP+ slots, NP7Lite and CP10 hardware accelerated, 480GB onboard SSD storage. |
| Transceivers | | |
| **1 GE SFP SX Transceiver Module** | FN-TRAN-SX | 1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| **1 GE SFP LX Transceiver Module** | FN-TRAN-LX | 1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| **10 GE SFP+ RJ45 Transceiver Module** | FN-TRAN-SFP+GC | 10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots. |
| **10 GE SFP+ Transceiver Module, Short Range** | FN-TRAN-SFP+SR | 10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots. |
| **10 GE SFP+ Transceiver Module, Long Range** | FN-TRAN-SFP+LR | 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots. |
| **10 GE SFP+ Transceiver Module, Extended Range** | FN-TRAN-SFP+ER | 10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots. |
| **10 GE SFP+ Transceiver Module, 80km Extreme Long Range** | FN-TRAN-SFP+ZR | 10GE SFP+ transceiver module, 80km extreme long range, for systems with SFP+ and SFP/SFP+ slots. |
| **10 GE SFP+ Transceiver Module, 30km Long Range** | FN-TRAN-SFP+BD27 | 10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately). |
| **10 GE SFP+ Transceiver Module, (connects to FN-TRAN-SFP+BD27, ordered separately)** | FN-TRAN-SFP+BD33 | 10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately). |
| **25 GE SFP28 Transceiver Module, Short Range** | FN-TRAN-SFP28-SR | 25 GE SFP28 transceiver module, short range, compatible with 10 GE SFP/SFP+ slots. |
| Cables | | |
| **10 GE SFP+ Passive Direct Attach Cable 1m** | FN-CABLE-SFP+1 | 10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots. |
| **10 GE SFP+ Passive Direct Attach Cable 3m** | FN-CABLE-SFP+3 | 10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots. |
| **10 GE SFP+ Passive Direct Attach Cable 5m** | FN-CABLE-SFP+5 | 10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots. |

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

April 30, 2025

FERTINET

Data Sheet

# FortiAnalyzer™

## Unified Data Lake, Visibility, and Automation

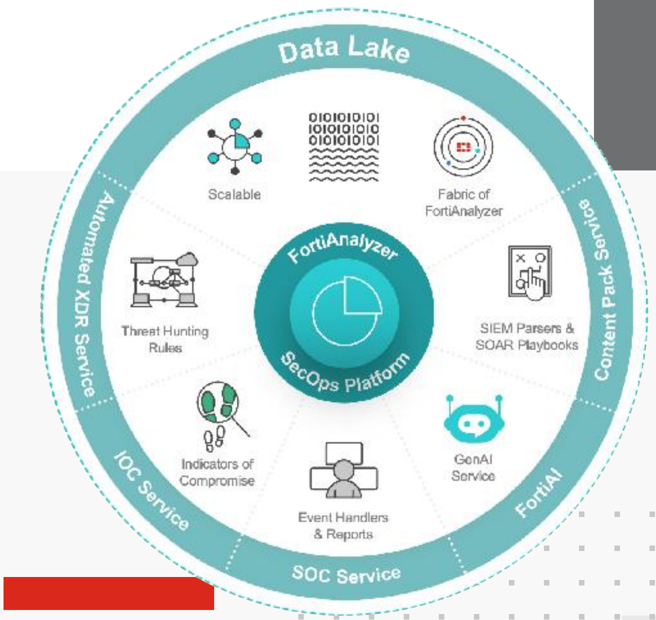
Available in:

Appliance

Virtual Machine

Cloud

Hosted



### Highlights

- Centralized log collection. Unified visibility across network and security assets
- Real-time system and network monitoring
- Prebuilt reports and dashboards
- Built-in SIEM and SOAR
- Advanced threat detection
- Regularly updated SOC Automation Content packs
- Generative AI assistant
- Built-in threat intelligence. Enriches events with real-time context from FortiGuard
- Scalable data lake and XDR-ready. Unified data lake connects events across endpoints, network and cloud
- Designed to complement and work alongside any SIEM or logging solution customers use

## FortiAnalyzer: The Turnkey Security Operations Platform

As the Data Lake of the Fortinet Security Fabric, FortiAnalyzer consolidates telemetry across networks, endpoints, and cloud environments, integrating Fortinet and third-party tools. It normalizes and enriches data with AI/ML-powered analytics, providing structured dashboards for IoT, SOC, email, and endpoint vulnerabilities. It streamlines operations with built-in threat intelligence, SIEM, and SOAR capabilities, along with prebuilt SOC automation content packs that are updated monthly. Enhanced with AI assistance and augmented operations delivered by FortiAI. Offering flexible deployment options across appliances, VMs, and the cloud, FortiAnalyzer enables network and security teams to detect faster, respond smarter, and improve efficiency—all from a single platform.

*Security teams are increasingly challenged to defend against complex and targeted threats — often with limited staff and resources.*

*FortiAnalyzer addresses this challenge by consolidating core SecOps capabilities into a single, turnkey platform that delivers a plug-and-play experience.*

*Designed for both on-premises and cloud environments, it eliminates the need for multiple security tools. This AI-driven solution empowers lean security teams to strengthen threat detection, automate incident response, and streamline critical security operations from one centralized platform.*

## Key Capabilities

### Unified Security Data Lake

*Centralized Visibility Across the Security Fabric*

FortiAnalyzer aggregates logs and telemetry from Fortinet products and third-party systems into a unified data lake. This centralized view enables better threat detection across networks, endpoints, applications, and cloud infrastructure and faster incident response.

Supports ingestion through various methods such as syslog, APIs, alert ingestion service, and agent-based forwarding using FortiClient. Offers scalable log storage with role-based access control and data retention policies to meet compliance requirements.

### Advanced Analytics and Correlation

*Detect Threats Earlier with Context-Rich Intelligence*

With built-in analytics and correlation across Security Fabric components, FortiAnalyzer helps identify sophisticated attacks by connecting seemingly unrelated events. Automated playbooks and event handlers improve response time and reduce manual workload.

### Real-Time Threat Intelligence

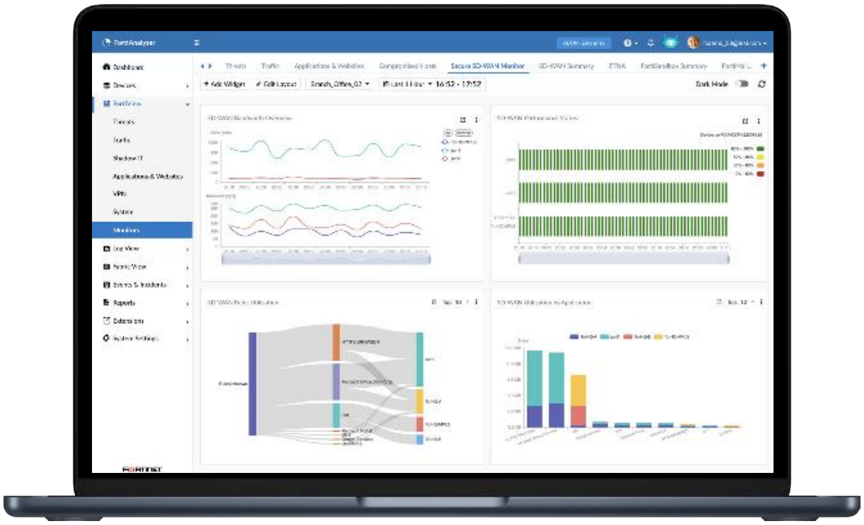
*Strengthen Detection with FortiGuard Feeds*

Integrates seamlessly with FortiGuard Labs' threat intelligence to enhance detection with the latest indicators of compromise, outbreak alerts service, enabling proactive defense and rapid investigation.

### Automation and Custom Reporting

*Operational Efficiency Through Automation*

Supports automated workflows for alert handling, ticketing, and notification. Built-in and Custom dashboards and compliance reports (e.g., PCI-DSS, HIPAA) provide actionable insights for both technical and executive audiences.



### Pre-Built Content Packs for SOC Automation

*Continuously Updated Intelligence to Accelerate SOC Operations*

FortiAnalyzer provides monthly content packs from FortiGuard Labs, delivering pre-built use cases that include log parsers, reports, correlation rules, event handlers, and automated playbooks. These content packs help organizations quickly onboard new log sources, detect emerging threats, and meet compliance requirements without extensive manual setup.

### Streamlined SOC Operations

*From Alert Monitoring to Automated Response*

FortiAnalyzer helps security operations centers manage the full incident lifecycle — from alert monitoring and triage to deep investigation and response. Analysts can efficiently prioritize alerts using built-in correlation, indicator enrichment, and user assets and identity tracking. Integrated connectors simplify data ingestion from Fortinet and third-party sources, while built-in playbooks and automation tools enable faster, consistent responses to common threats.

### Generative AI Assistant for Faster Insights

*Simplifying Investigations and Enhancing Analyst Efficiency*

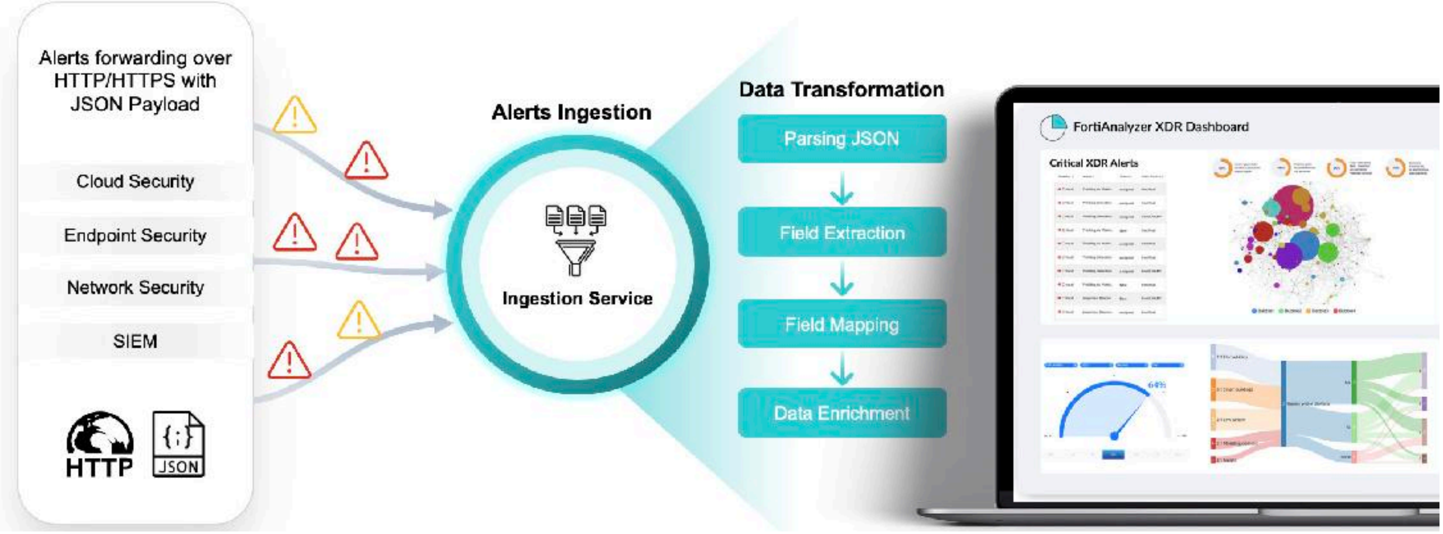
FortiAnalyzer includes a built-in Generative AI assistant that helps security teams quickly analyze and understand complex data. Analysts can use natural language queries to explore logs, summarize incidents, or ask questions about alerts—without needing deep query language expertise. The AI assistant provides context-aware insights, speeds up investigations, and reduces time spent on manual data correlation. Integrated with the Security Fabric, it helps SOC teams make faster, more informed decisions across a broad range of security events.

### Extended Detection and Response Across the Security Fabric

*Coordinated Detection and Response Across Multiple Security Layers*

FortiAnalyzer enables extended detection and response (XDR) by integrating with key Fabric SecOps platforms such as FortiEDR, FortiNDR, FortiDeceptor, FortiCNAPP, and FortiDLP. It correlates data across these layers to deliver unified visibility, advanced threat detection, and enriched context for faster investigations.

Automated responses can be triggered through integrated enforcement points such as FortiGate, FortiManager, FortiMail, FortiEDR, FortiAuthenticator and FortiCNAPP — enabling quick containment, policy enforcement, or remediation actions. This tightly integrated approach helps SOC teams detect threats earlier, respond faster, and reduce risk across endpoints, networks, applications, and the cloud.



### High Availability and Scalable Fabric Architecture

*Resilient and Distributed for Enterprise and Hyperscale Environments*

- **Flexible Deployment Options**

FortiAnalyzer supports a wide range of deployment models to fit diverse infrastructure needs, offering adaptability across on-premises, cloud, and hybrid environments. It is available as a physical appliance for on-premises deployments, a virtual appliance for private or public cloud environments, and also as a hosted solution. This flexibility enables easy scalability across branch offices, hybrid cloud setups, and centralized Security Operations Centers (SOCs).

- **FortiAnalyzer High Availability (HA)**

FortiAnalyzer HA provides real-time redundancy to protect organizations by ensuring continuous operational availability. In the event that the primary (active) FortiAnalyzer fails, a secondary (passive) FortiAnalyzer (up to four-node cluster) will immediately take over, providing log and data reliability and eliminating the risk of having a single point of failure.

- **FortiAnalyzer Fabric**

FortiAnalyzer Fabric allows SOC Administrators to configure two operation modes - Supervisor and Member. This allows viewing of member devices, ADOMs and authorized logging devices, as well as incidents and events created on members. Admins get access to Reports and FortiView across all member FortiAnalyzers, and can perform global search in Log View of logs collected across FortiAnalyzer Fabric members with pre-defined device filters and log drill down for each Member and Member ADOMs.

- **Analyzer Collector Modes**

FortiAnalyzer provides two operation modes: Analyzer and Collector. In Collector mode, the primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. This configuration greatly benefits organizations with increasing log rates, as the resource intensive log-receiving task is off-loaded to the Collector so that the Analyzer can focus on generating analytics and reports.

Network operations teams can deploy multiple FortiAnalyzers in Collector and Analyzer modes to work together to improve the overall performance of log receiving and processing increased log volumes, providing log storage and redundancy, and rapid delivery of critical network and threat information.

- **Log Forwarding for Third-Party Integration**

Forward logs from one FortiAnalyzer to another FortiAnalyzer unit, a syslog server, or (CEF) server. In addition to forwarding logs to another unit or server, the client FortiAnalyzer retains a local copy of the logs, which are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received from network devices.

## Subscriptions and Extensions

### Subscription Licenses and FortiGuard Security Services

- **FortiGuard Outbreak Detection Service**

Deliver automated content package download for detecting the latest malware, including a summary of outbreaks and kill chain mapping for how the malware works. The package includes a FortiGuard Report for the outbreak, Event Handler, and a Report Template to detect outbreaks.

- **FortiGuard Indicators of Compromise Service**

Empower security teams with forensic data from 500 000 IOCs daily, used in combination with FortiAnalyzer analytics to identify suspicious usage and artifacts observed on the network or in an operations system, that have been determined with high confidence to be malicious infections or intrusions, and historical rescan of logs for threat hunting.

- **OT Security Service**

Provide security teams with advanced OT analytics, risk and compliance reports, OT event handlers, and use-case correlation rules.

- **FortiAnalyzer Attack Surface Security Rating and Compliance Service**

Helps security teams design, implement, and maintain their security posture, and provides actionable configuration recommendations as well as key performance and risk indicators

.

- **SOC Automation Subscription Service**

Subscription enables further automation for incident response with enhanced monitoring and escalation, built-in incident management workflows, connectors, playbooks and more.

- **FortiAI Subscription Service**

Provide a generative AI security assistant integrated into FortiAnalyzer for incident investigation, response, and threat hunting. It interprets security events, generates summaries, identifies potential impacts, and offers remediation recommendations. By using natural language prompts, FortiAI can create complex database queries, generate reports, and efficiently perform various other FortiAnalyzer functions.

# Cloud Services

### FortiAnalyzer Cloud

FortiAnalyzer Cloud offers customers a PaaS-based delivery option for automation-driven, single pane analytics, providing log management, analytics, and reporting for Fortinet NGFW and SD-WAN with an easily accessible cloud-based solution. FortiAnalyzer Cloud delivers reliable real-time insights into network activity with extensive reporting and monitoring for clear, consistent visibility of an organization's security posture. Customers can easily access their FortiAnalyzer Cloud from their FortiCloud single sign-on portal.

# Virtual Offerings

### FortiAnalyzer VM Subscription

The FortiAnalyzer VM Subscription license model consolidates into one single SKU: VM product SKU, FortiCare Support SKU, FortiGuard IOC and Outbreak Detection Service, SOC Automation services, to simplify the product purchase, upgrade, and renewal. FortiAnalyzer-VM S provides organizations with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining, and vulnerability assessment. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet and third party devices deliver a simplified, consolidated view of your security posture.

The FortiAnalyzer-VM S series SKUs come in stackable 5, 50, and 500 GB/ day logs licenses, so that multiple units of this SKU can be purchased together providing organizations with the ability and cost-efficiencies to scale and meet their logging needs.

### FortiAnalyzer VM

Fortinet offers FortiAnalyzer-VM licensing in a perpetual license model with a-la-carte technical support and subscription services. This software-based version of the FortiAnalyzer hardware appliance is designed to run on many virtualization platforms, allowing you to expand your virtual solution as your environment expands.

| FORTIANALYZER VIRTUAL APPLIANCES | FAZ-VM-GB1 | FAZ-VM-GB5 | FAZ-VM-GB25 | FAZ-VM-GB100 | FAZ-VM-GB500 | FAZ-VM-GB2000 |
|---|---|---|---|---|---|---|
| **Capacity** | | | | | | |
| **GB/ day of Logs *** | +1 | +5 | +25 | +100 | +500 | +2000 |
| **Devices/VDOMs Maximum** | 10 000 | 10 000 | 10 000 | 10 000 | 10 000 | 10 000 |
| **FortiGuard IOC Service** | ✓ | | | | | |
| **Security Automation Service** | ✓ | | | | | |
| **Hypervisor Support** | Up-to-date hypervisor support can be found in the release note for each FortiAnalyzer version. Visit https://docs.fortinet.com/product/fortianalyzer/ and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiAnalyzer [version] support" → "Virtualization" | | | | | |
| **vCPU Support (Minimum / Maximum)** | 4 / Unlimited | | | | | |
| **Network Interface Support (Min / Max) **** | 1 / 12 | | | | | |
| **Memory Support (Minimum / Maximum)** | 16 GB / Unlimited for 64-bit | | | | | |

* Unlimited GB/ day when deployed in collector mode.

** VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms.

# Specifications

| FORTIANALYZER APPLIANCES | FAZ-150G | FAZ-300G | FAZ-810G | FAZ-1000G |
|---|---|---|---|---|
| **Capacity and Performance** | | | | |
| **GB/ day of Logs** | 25 | 100 | 200 | 660 |
| **Analytic Sustained Rate (logs/ sec)*** | 500 | 2000 | 4000 | 20 000 |
| **Collector Sustained Rate (logs/ sec)*** | 750 | 3000 | 6000 | 30 000 |
| **Devices/VDOMs (Maximum)** | 50 | 180 | 800 | 2000 |
| **Max Number of Days Analytics**** | 90 | 50 | 50 | 60 |
| **Options** | | | | |
| **FortiGuard IOC and Outbreak Detection Service** | ✓ | ✓ | ✓ | ✓ |
| **SOC Automation Service** | ✓ | ✓ | ✓ | ✓ |
| **Enterprise Bundle** | ✓ | ✓ | ✓ | ✓ |
| **Hardware Bundle** | ✓ | ✓ | ✓ | ✓ |
| **OT Security Service** | ✓ | ✓ | ✓ | ✓ |
| **Security Rating and Compliance Service** | ✓ | ✓ | ✓ | ✓ |
| **Hardware Specifications** | | | | |
| **Form Factor (supports EIA/non-EIA standards)** | Desktop | 1 RU Rackmount | 1 RU Rackmount | 2 RU Rackmount |
| **Total Interfaces** | 2x RJ45 GE | 4x RJ45 GE | 4x RJ-45 2x GE SFP | 2× 2.5GbE RJ45 + 2× 25GbE SFP28 |
| **Storage Capacity** | 4TB (2× 2TB) | 8 TB (2× 4 TB) | 16TB (4× 4TB) 3.5 in SAS HDDs | 32 TB (8 × 4TB) 3.5 in SAS SED HDD |
| **Usable Storage (After RAID)** | 2 TB | 4 TB | 8 TB | 24 TB |
| **Removable Hard Drives** | No | No | ✓ | ✓ |
| **RAID Levels Supported** | 0/1 | RAID 0/1 | RAID 0/1,1s/5,5s/10 | RAID 0/1/5/6/10/50/60 |
| **RAID Type** | Software | Software | Hardware / Hot Swappable | Hardware / Hot Swappable |
| **Default RAID Level** | 1 | 1 | 10 | 50 |
| **Redundant Hot Swap Power Supplies** | No | Optional | Optional | ✓ |
| **Trusted Platform Module (TPM) ***** | Gen 2 | Gen 2 | ✓ | ✓ |
| **Dimensions** | | | | |
| **Height x Width x Length (inches)** | 9.5 × 3.5 × 8 | 1.73 × 17.24 × 16.38 | 1.73 × 17.32 × 21.65 | 3.46 × 17.24 × 24.41 |
| **Height x Width x Length (cm)** | 24.1 × 8.9 × 20.55 | 4.4 × 43.8 × 41.6 | 4.4 × 44.0 × 55.0 | 8.8 × 43.8 × 62.0 |
| **Weight** | 9.35 lbs (4.24 kg) | 22.5 lbs (10.2 kg) | 25.75 lbs (11.68 kg) | 49.6 lbs (22.5 kg) |
| **Environment** | | | | |
| **AC Power Supply** | 100–240V AC, 50–60 Hz | 100–240V AC, 60–50 Hz | 100-240Vac, 50~60Hz, 4A max | 100-240Vac, 50~60Hz, 4A max |
| **Power Consumption (Average / Maximum)** | 36 W / 43 W | 90.1 W / 99 W | 115W / 150W | 251.36W / 302W |
| **Heat Dissipation** | 147.4 BTU/h | 337.8 BTU/h | 433 BTU/h | 857.73 BTU/h |
| **Operating Temperature** | 32°F to 104° F (0°C to 40° C) | 32°F to 104° F (0°C to 40° C) | 32°F to 104° F (0°C to 40° C) | 32°F to 104° F (0°C to 40° C) |
| **Storage Temperature** | -4°F to 167° F (-20°C to 75° C) | -13°F to 167° F (-25°C to 75° C) | -4°F to 167° F (-20°C to 75° C) | -40°F to 158° F (-40°C to 70° C) |
| **Humidity** | 5% to 95% non-condensing | 20% to 90% non-condensing | 5% to 95% non-condensing | 5% to 95% non-condensing |
| **Forced Airflow** | Front to Back | Front to Back | Front to Back | Front to Back |
| **Operating Altitude** | Up to 7400 ft (2250 m) | Up to 7400 ft (2250 m) | Up to 7400 ft (2250 m) | Up to 16 404 ft (5000 m) |
| **Compliance** | | | | |
| **Safety Certifications** | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB |

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** The maximum number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

# Specifications

| FORTIANALYZER APPLIANCES | FAZ-3100G | FAZ-3510G | FAZ-3700G |
|---|---|---|---|
| **Capacity and Performance** | | | |
| **GB/ day of Logs** | 3000 | 5000 | 8300 |
| **Analytic Sustained Rate (logs/sec)*** | 42 000 | 60 000 | 100 000 |
| **Collector Sustained Rate (logs/sec)*** | 60 000 | 90 000 | 150 000 |
| **Devices/VDOMs (Maximum)** | 4000 | 10 000 | 10 000 |
| **Max Number of Days Analytics**** | 30 | 35 | 60 |
| **Options** | | | |
| **FortiGuard IOC and Outbreak Detection Service** | ✓ | ✓ | ✓ |
| **Security Automation Service** | ✓ | ✓ | ✓ |
| **Enterprise Bundle** | ✓ | ✓ | ✓ |
| **Hardware Bundle** | ✓ | ✓ | ✓ |
| **OT Security Service** | ✓ | ✓ | ✓ |
| **Security Rating and Compliance Service** | ✓ | ✓ | ✓ |
| **Hardware Specifications** | | | |
| **Form Factor (supports EIA/non-EIA standards)** | 3 RU Rackmount | 4 RU Rackmount | 4 RU Rackmount |
| **Total Interfaces** | 2x GE RJ45, 2× 25GE SFP28 | 2× 10GbE RJ45, 2× 25GbE SFP28 | 2× 10GE RJ-45 + 2× 25GE SFP28 |
| **Storage Capacity** | 64 TB (16 × 4TB) 3.5" SAS SED HDD + 3.84 (2× 1.92TB) 2.5" NVMe SSD | 24× 4TB (96TB) + 2× 3.84TB (7.68TB) | 240TB (60× 4TB) 3.5 in HDD + 19.2TB (6× 3.2TB) NVMe SSD |
| **Usable Storage (After RAID)** | 56 TB | 84 TB | 224 TB |
| **Removable Hard Drives** | ✓ | ✓ | ✓ |
| **RAID Levels Supported** | RAID 0/1,1s/5,5s/6,6s/10/50/60 | RAID 0/1,1s/5,5s/6,6s/10/50/60 | RAID 0/1,1s/5,5s/6,6s/10/50/60 |
| **RAID Type** | Hardware / Hot Swappable | Hardware / Hot Swappable | Hardware / Hot Swappable |
| **Default RAID Level** | 50 | 50 | 50 |
| **Redundant Hot Swap Power Supplies** | ✓ | ✓ | ✓ |
| **Trusted Platform Module (TPM) ***** | ✓ | ✓ | ✓ |
| **Dimensions** | | | |
| **Height x Width x Length (inches)** | 5.2 × 17.2 × 25.5 | 7 × 17.2 × 27.5 | 7.0 × 17.2 × 30.2 |
| **Height x Width x Length (cm)** | 13.0 × 44.0 × 65.0 | 17.8 × 43.7 × 69.9 | 17.8 × 43.7 × 76.7 |
| **Weight** | 69.6 lbs (31.57 kg) | 65 lbs (29.5 kg) | 118 lbs (53.5 kg) |
| **Environment** | | | |
| **AC Power Supply** | 100-127V~/10A, 200-240V~/5A | 100-127V~/10A, 200-240V~/5A | 2000W AC**** |
| **Power Consumption (Average/Max)** | 395 W / 510 W | 983 W / 1278 W | 850 W / 1423.4 W |
| **Heat Dissipation** | 1740.19 BTU/h | 3424 BTU/h | 4858 BTU/h |
| **Operating Temperature** | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) | 50°F to 95°F (10°C to 35°C) |
| **Storage Temperature** | -4°F to 158°F (-20°C to 70°C) | -4°F to 167°F (-20°C to 75°C) | -40°F to 158°F (-40°C to 70°C) |
| **Humidity** | 5% to 95% (non-condensing) | 5% to 95% (non-condensing) | 8% to 90% (non-condensing) |
| **Forced Airflow** | Front to Back | Front to Back | Front to Back |
| **Operating Altitude** | Up to 13 123 ft (4000 m) | Up to 10 000 ft (3048 m) | Up to 7400 ft (2250 m) |
| **Compliance** | | | |
| **Safety Certifications** | FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB | FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB | FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB |

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** is the max number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

****3700G must connect to a 200V - 240V power source.

## Ordering Information

| Product | SKU | Description |
|---|---|---|
| **FortiAnalyzer** | FAZ-150G | Centralized log and analysis appliance — 2x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs. |
| | FAZ-300G | Centralized log and analysis appliance — 4x RJ45 GE, 8 TB storage, up to 100 GB/ day of logs. |
| | FAZ-810G | Centralized log and analysis appliance — 4x GE, 2x SFP, 16 TB self-encrypting storage, up to 200 GB/ day of logs. |
| | FAZ-1000G | Centralized logging and analysis appliance - 2× 2.5GbE RJ45 + 2× 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs. |
| | FAZ-3100G | Centralized log and analysis appliance — 2x GE RJ45, 2× 25GE SFP28, 64 TB storage, dual power supplies, up to 3000 GB/ day of logs. |
| | FAZ-3510G | Centralized log and analysis appliance — 2× 10GbE RJ45, 2× 25GbE SFP28, 96 TB storage, up to 5000 GB/ day of logs. |
| | FAZ-3700G | Centralized log and analysis appliance - 2× 10GE RJ-45 + 2× 25GE SFP28 slots, 240TB HDD + 19.2TB NVMe SSD storage, up to 8300 GB/ day of Logs. |
| **FortiAI Subscription** | FC-10-[Model Code]-1118-02-DD | Generative AI powered security service utilizing large language models (LLMs) for real-time assistance in SOC analysis, incident investigation, triage and response. |
| **FortiAnalyzer-VM Subscription License with Support** | FC1-10-AZVMS-465-01-DD | Subscription license for 5 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service. |
| | FC2-10-AZVMS-465-01-DD | Subscription license for 50 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service. |
| | FC3-10-AZVMS-465-01-DD | Subscription license for 500 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service. |
| **FortiAnalyzer-VM** | FAZ-VM-GB1 | Upgrade license for adding 1 GB/Day of Logs. |
| | FAZ-VM-GB5 | Upgrade license for adding 5 GB/Day of Logs. |
| | FAZ-VM-GB25 | Upgrade license for adding 25 GB/Day of Logs. |
| | FAZ-VM-GB100 | Upgrade license for adding 100 GB/Day of Logs. |
| | FAZ-VM-GB500 | Upgrade license for adding 500 GB/Day of Logs. |
| | FAZ-VM-GB2000 | Upgrade license for adding 2 TB/Day of Logs. |
| **FortiAnalyzer Cloud Storage Subscription** | FC1-10-AZCLD-463-01-DD | Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service. |
| | FC2-10-AZCLD-463-01-DD | Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service. |
| | FC3-10-AZCLD-463-01-DD | Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service. |
| **FortiAnalyzer - Backup to Cloud Service** | FC-10-FAZ00-286-02-DD | One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud. |
| **SOCaaS** | FC-10-[Model Code]-464-02-DD | SOCaaS: 24×7 cloud-based managed log monitoring, incident triage and SOC escalation service. |
| **FortiAnalyzer Cloud** | FC-10-[Model Code]-585-02-DD | FortiAnalyzerCloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service. |
| **Security Automation Service** | FC-10-[Model Code]-335-02-DD | Subscription license for Security Automation Service - Appliance. |
| | FC[GB Day Code]-10-LV0VM-335-02-DD | Subscription license for Security Automation Service - Virtual Machine. |
| **FortiGuard IOC and Outbreak Detection Service** | FC-10-[Model Code]-661-02-DD | Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance. |
| | FC[GB Day Code]-10-LV0VM-661-02-DD | Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine. |
| **OT Security Service** | FC-10-[Model Code]-159-02-DD | OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules. |
| **FortiAnalyzer Security Rating and Compliance Service** | FC-10-[Model Code]-175-02-DD | Subscription license for FortiAnalyzer Security Rating and Compliance Service. |
| **Enterprise Protection Bundle** | FC-10-[Model Code]-466-02-DD | Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service). |
| **Hardware Bundle** | FAZ-[Hardware Model]-BDL-466-DD | Hardware plus FortiCare Premium and FortiAnalyzer Enterprise Protection. |

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

April 4, 2025

FORTINET

Data Sheet

# FortiWeb™

**Available in**

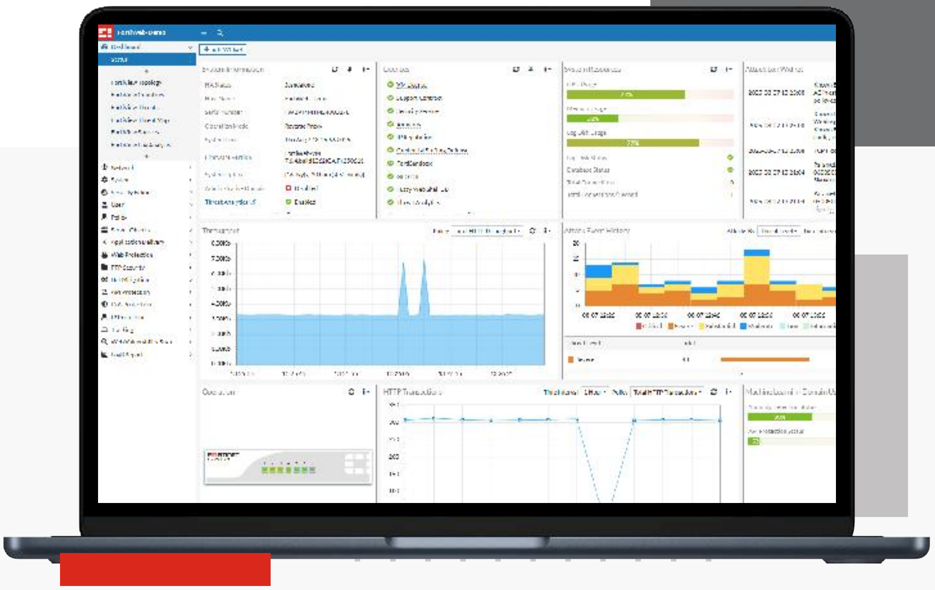
Appliance

Virtual

SaaS

Cloud

Container



### Highlights

Machine learning that detects and blocks threats while minimizing false positives

Advanced Bot Mitigation effectively protect web assets without imposing friction on legitimate users

Protection for APIs, including those used to support mobile applications

Enhanced protection with Fortinet Security Fabric integration

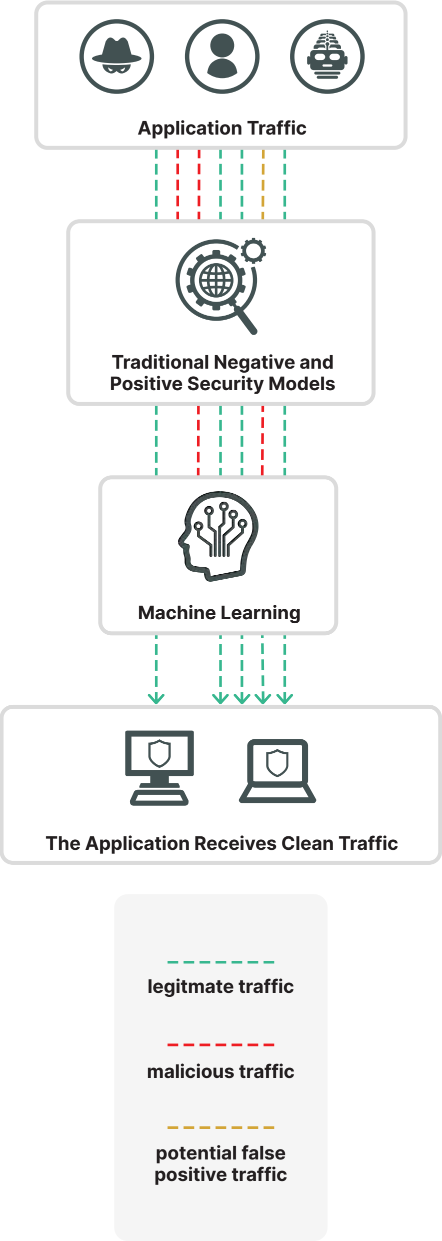
Simplified attack investigation with Threat Analytics

Third-party integration and virtual patching

## Web Application and API Protection

FortiWeb is a web application firewall (WAF) that protects web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations.

Using machine learning to model each application, FortiWeb defends applications from known vulnerabilities and from zero-day threats. High performance physical, virtual appliances, and containers deploy on-site or in the public cloud to serve any size of the organization—from small businesses to service providers, carriers, and large enterprises.


Application Traffic
Traditional Negative and Positive Security Models
Machine Learning
The Application Receives Clean Traffic
legitimate traffic
malicious traffic
potential false positive traffic

FortiWeb goes beyond traditional negative and positive security models (such as attack signatures, IP address reputation, and protocol validation), and applies a second layer of machine learning-based analytics to detect and block malicious anomalies while minimizing false positives.

## Highlights

### Comprehensive Web Application Security

Using an advanced multi-layered and correlated approach, FortiWeb provides complete security for your web-based applications from the OWASP Top 10 and many other threats. FortiWeb's first layer of defense uses traditional WAF detection engines (e.g. attack signatures, IP address reputation, protocol validation, and more) to identify and block malicious traffic, powered by intelligence from Fortinet's industry leading security research from FortiGuard Labs. FortiWeb's machine learning detection engine then examines traffic that passes this first layer, using a continuously updated model of your application to identify malicious anomalies and block them as well.

### API Discovery and Protection

Fueling the digital transformation APIs have become increasingly popular, providing the backbone for mobile applications, automated business to business operations and ease of management across applications. However, with their popularity they also increase the attack surface with additional exposed application surfaces that organizations must secure. Fortinet's FortiWeb web application firewall provides the right tools to address threats to APIs. FortiWeb API Discovery and Protection uses machine learning algorithms to automatically discover APIs by continuously evaluating application traffic. Discovery is an integral role for establishing a positive security model and FortiWeb protects your critical APIs based on your profiled API inventory. FortiWeb can also integrate out of the box policies together with an automatically generated positive security model policy that is based on your organization's schema specification (OpenAPI, XML and generic JSON are supported schemas) to protect against API exploits. FortiWeb schema validation can be integrated into the CI/CD pipeline, automatically generating an updated positive security model policy once the API is updated.

### Bot Mitigation

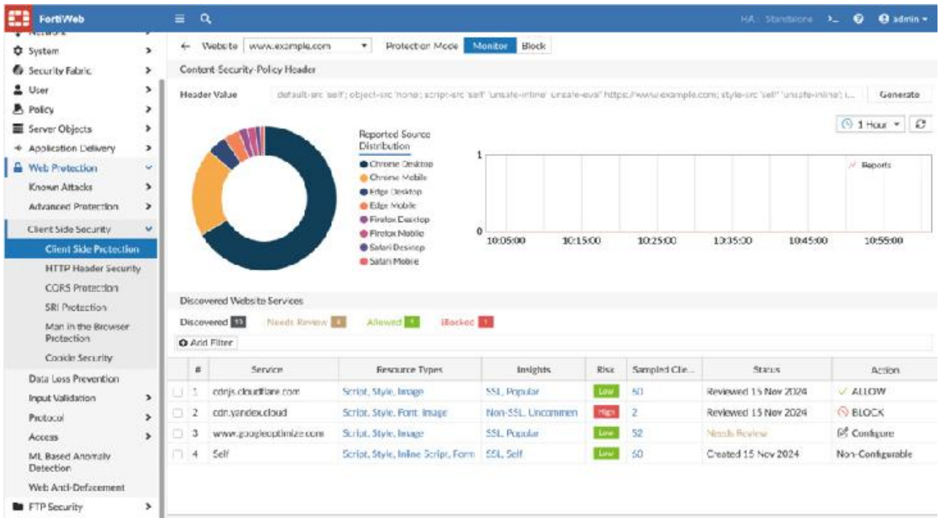
FortiWeb protects against automated bots, webs scrapers, crawlers, data harvesting, credential stuffing and other automated attacks to protect your web assets, mobile APIs, applications, users and sensitive data. Combining machine learning with policies such as threshold based detection, Bot deception and Biometrics based detection with superior good bot identification FortiWeb is able to block malicious bot attacks while reducing friction on legitimate users. With advanced tracking techniques FortiWeb can differentiate between humans, automated requests and repeat offenders, track behavior over time to better identify humans from bots and enforce CAPTCHA challenges when required. Together with FortiView, FortiWeb's graphical analysis dashboard organizations can quickly identify attacks and differentiate from good bots and legitimate users.

# Highlights

### Client-Side Protection (PCI DSS 4.0 Compliance)

FortiWeb Client-Side Protection continuously detects and blocks malicious and unauthorized JavaScript running in users' browsers, providing real-time visibility and robust security for your websites—without impacting performance. The solution defends against threats like formjacking, Magecart, and online skimming, helping to safeguard sensitive customer data. Security teams gain detailed monitoring, activity alerts, and control over both first- and third-party scripts, streamlining incident response.

Designed to support PCI DSS 4.0 compliance, FortiWeb Client-Side Protection addresses key requirements by inventorying, authorizing, and monitoring all scripts on payment pages, in line with mandates such as requirements 6.4.3 and 11.6.1. This solution enables real-time script integrity checking and simplifies compliance reporting, ensuring only approved scripts run on sensitive web pages and helping organizations efficiently meet new client-side security obligations.



Website: www.example.com

Protection Mode: Monitor

Content Security Policy Header

Header Value: default-src 'self'; object-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.example.com; style-src 'self' 'unsafe-inline'; i...

Discovered Website Services

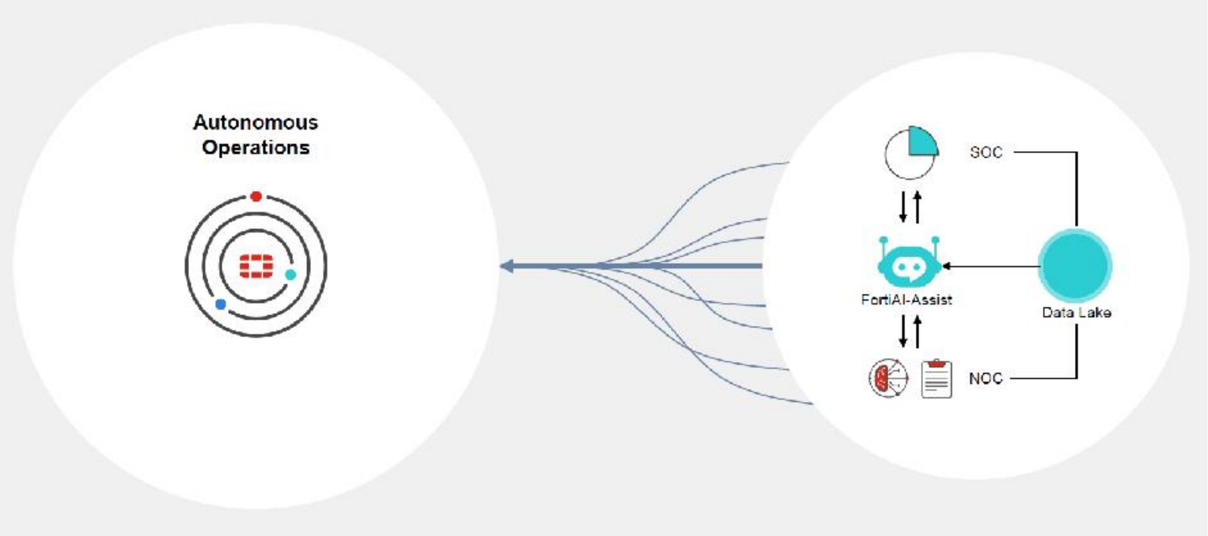
| # | Service | Resource Types | Insights | Risk | Sampled Cle... | Status | Action |
|---|---|---|---|---|---|---|---|
| 1 | cdnjs.cloudflare.com | Script, Style, Image | SSL, Popular | Low | 60 | Reviewed 15 Nov 2024 | ✓ ALLOW |
| 2 | cdn.yandex.cloud | Script, Style, Font, Image | Non-SSL, Uncommon | High | 2 | Reviewed 15 Nov 2024 | BLOCK |
| 3 | www.googleoptimize.com | Script, Style, Image | SSL, Popular | Low | 52 | Needs Review | Configure |
| 4 | Self | Script, Style, Inline Script, Form | SSL, Self | Low | 60 | Created 15 Nov 2024 | Non-Configurable |

### FortiAI-Assist

FortiAI-Assist automates security tasks, from policy updates to configuration corrections. It optimizes network operations and provides quick answers to questions on specifications, deployment methods, and feature configurations. Alert triage prioritizes high-risk threats, suppressing duplicates. Adaptive threat hunting scans for threats without human input. Root-cause tracing identifies attack origins, while threat intelligence enrichment improves proactive defense. FortiAI-Assist streamlines operations, strengthens security, and reduces manual effort.

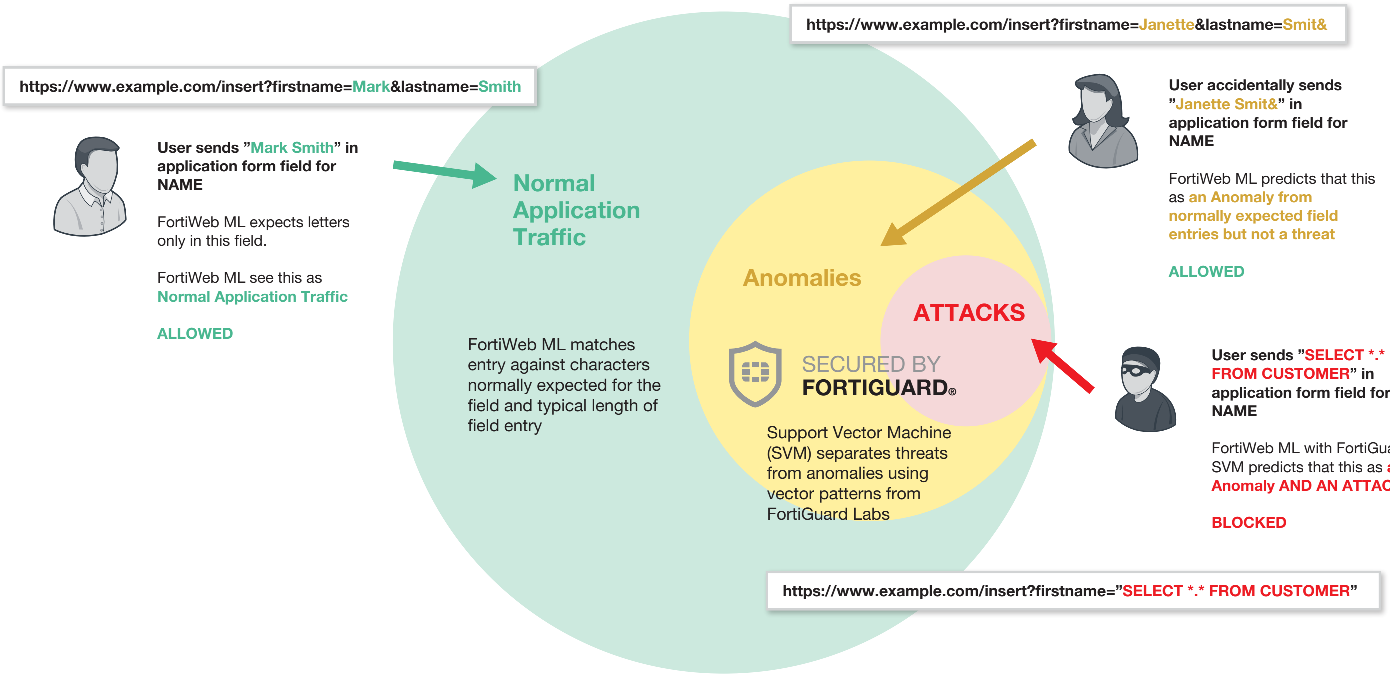
## FortiAI-Assist: Leverage GenAI and Agentic AI

### Predictive, proactive, and adaptive towards an autonomous network



## Highlights

FortiWeb's machine learning accurately detects anomalies and identifies which are threats. Unlike prevailing auto-learning detection models used by other WAF vendors that treat every anomaly as a threat, FortiWeb's precision nearly eliminates false positive detections and catches attack types that others cannot.



https://www.example.com/insert?firstname=Mark&lastname=Smith

User sends "Mark Smith" in application form field for NAME

FortiWeb ML expects letters only in this field.

FortiWeb ML see this as Normal Application Traffic

ALLOWED

FortiWeb ML matches entry against characters normally expected for the field and typical length of field entry

https://www.example.com/insert?firstname=Janette&lastname=Smit&

User accidentally sends "Janette Smit&" in application form field for NAME

FortiWeb ML predicts that this as an Anomaly from normally expected field entries but not a threat

ALLOWED

Support Vector Machine (SVM) separates threats from anomalies using vector patterns from FortiGuard Labs

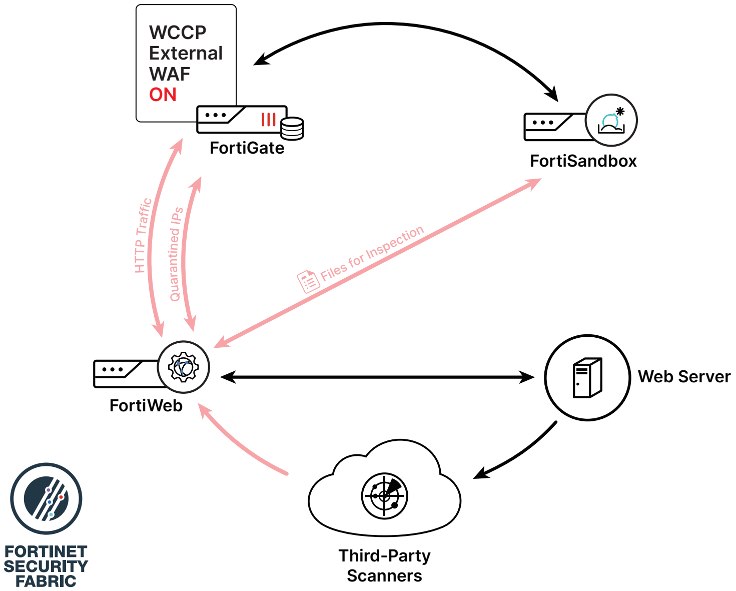
User sends "SELECT *.* FROM CUSTOMER" in application form field for NAME

FortiWeb ML with FortiGuard SVM predicts that this as an Anomaly AND AN ATTACK

BLOCKED

https://www.example.com/insert?firstname="SELECT *.* FROM CUSTOMER"

FortiWeb's AI-based machine learning evaluates application requests to determine if they are normal, benign anomalies, or anomalies that are threats.



Integration with other Fortinet Security Fabric elements, including FortiGate and FortiSandbox, delivers APT protection and extends vulnerability scanning with leading third-party providers.

### Deep Integration into the Fortinet Security Fabric and Third-Party Scanners

As the threat landscape evolves, many new threats require a multi-pronged approach for protecting web-based applications. Advanced Persistent Threats that target users can take many different forms than traditional single-vector attack types and can evade protections offered only by a single device. FortiWeb's integration with FortiGate and FortiSandbox extend basic WAF protections through synchronization and sharing of threat information to both deeply scan suspicious files and share infected internal sources.

FortiWeb also provides integration with leading third-party vulnerability scanners including Acunetix, HP WebInspect, IBM AppScan, Qualys, ImmuniWeb and WhiteHat to provide dynamic virtual patches to security issues in application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules by FortiWeb to protect the application until developers can address them in the application code.

## Highlights

### Solving the Challenge of False Threat Detections

False positive threat detections can be very disruptive and force many administrators to loosen security rules on their web application firewalls to the point where many often become a monitoring tool rather than a trusted threat avoidance platform. The installation of a WAF may take only minutes, however fine-tuning can take days, or even weeks. Even after setup, a WAF can require regular checkups and tweaks as applications and the environment change.

FortiWeb's AI-based machine learning addresses false positive and negative threat detections without the need to tediously manage whitelists and fine-tune threat detection policies. With near 100% accuracy, the dual layer machine learning engines detect anomalies and then determine if they are threats unlike other methods that block all anomalies regardless of their intent. When combined with other tools, including user tracking, session tracking, and threat weighting, FortiWeb virtually eliminates all false detection scenarios.

### Advanced Graphical Analysis and Reporting

FortiWeb includes a suite of graphical analysis tools called FortiView. Similar to other Fortinet products such as FortiGate, FortiWeb gives administrators the ability to visualize and drill-down into key elements of FortiWeb such as server/IP configurations, attack and traffic logs, attack maps, OWASP Top 10 attack categorization, and user activity. FortiView for FortiWeb lets administrators quickly identify suspicious activity in real time and address critical use cases such as origin of threats,  common violations, and client/device risks.

### Secured by FortiGuard

Fortinet's Award-winning FortiGuard Labs is the backbone for many of FortiWeb's layers in its approach to application security. Offered as five separate options, you can choose the FortiGuard services you need to protect your web applications. FortiWeb IP address reputation service protects you from known attack sources like botnets, spammers, anonymous proxies, and sources known to be infected with malicious software.

FortiWeb Security Service is designed just for FortiWeb including items such as application layer signatures, machine learning threat models, malicious robots, suspicious URL patterns, and web vulnerability scanner updates. Credential Stuffing Defense checks login attempts against FortiGuard's list of compromised credentials and can take actions ranging from alerts to blocking logins from suspected stolen user ids and passwords. The FortiWeb Cloud Sandbox subscription enables FortiWeb to integrate with Fortinet's cloud-sandbox service. Finally, FortiWeb offers FortiGuard's top-rated antivirus engine that scans all file uploads for threats that can infect your servers or other network elements.

### VM and Public Cloud Options

FortiWeb provides maximum flexibility in supporting your virtual and hybrid environments. The virtual versions of FortiWeb support all the same features as our hardware-based devices and can be deployed in VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, and Docker platforms. FortiWeb is also available for AWS, Azure, Google Cloud, and Oracle Cloud as a VM, and as WAF as a Service. For more information, see Fortiweb-Cloud.com.

# Features

### Deployment Options

- Reverse Proxy
- Inline Transparent
- True Transparent Proxy
- Offline Sniffing
- WCCP

### Web Security

- AI-based Machine Learning
- Automatic profiling (white list)
- Web server and application signatures (black list)
- IP address reputation
- IP address geolocation
- HTTP RFC compliance
- Native support for HTTP/2
- WebSocket protection and signature enforcement
- Man in the Browser (MiTB) protection
- Client-Side Protection

### Application Attack Protection

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking
- Built-in Vulnerability Scanner
- Third-party scanner integration (virtual patching)
- File upload scanning with AV and sandbox

### Security Services

- Malware detection
- Virtual patching
- Protocol validation
- Brute force protection
- Cookie signing and encryption
- Threat scoring and weighting
- Syntax-based SQLi and XSS detection
- HTTP Header Security
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- L4 Stateful Network Firewall
- DoS prevention
- Advanced correlation protection using multiple security elements
- Data leak prevention
- Web Defacement Protection

### Application Delivery

- Layer 7 server load balancing
- URL Rewriting
- Content Routing
- HTTPS/SSL Offloading
- HTTP Compression
- Caching

### Authentication

- Active and passive authentication
- Site Publishing and SSO
- RSA Access for 2-factor authentication
- LDAP, RADIUS, and SAML support
- SSL client certificate support
- CAPTCHA and Real Browser Enforcement (RBE)

### API Protection

- Machine Learning based API Discovery and Protection
- XML and JSON protocol conformance
- CI/CD integration
- Schema verification
- API Gateway
- Web services signatures

### Bot Mitigation

- Machine Learning based Bot Mitigation
- Biometrics Based Detection
- Threshold Based Detection
- Bot Deception
- Know Bots

### Management and Reporting

- Web user interface
- Command line interface
- FortiView graphical analysis and reporting tools
- Central management for multiple FortiWeb devices
- Active/Active HA Clustering
- REST API
- Centralized logging and reporting
- User/device tracking
- Real-time dashboards
- Bot dashboard
- OWASP Top 10 attack categorization
- Geo IP Analytics
- SNMP, Syslog and Email Logging/Monitoring
- Administrative Domains with full RBAC

### Other

- IPv6 Ready
- HTTP/2 to HTTP 1.1 translation
- HSM Integration
- Seamless PKI integration
- Attachment scanning for ActiveSync/MAPI applications, OWA, and FTP
- High Availability with Config-sync for syncing across multiple active appliances
- Auto setup and default configuration settings for simplified deployment
- Setup Wizards for common applications and databases
- Preconfigured for common Microsoft applications; Exchange, SharePoint, OWA
- OpenStack support for FortiWeb VMs
- Predefined security policies for Drupal and Wordpress applications
- WebSockets support

## Specifications

| | FORTIWEB 100F | FORTIWEB 400F | FORTIWEB 600F |
|---|---|---|---|
| **Hardware** | | | |
| **10/100/1000 Interfaces (RJ-45 ports)** | 4 | 4 GE RJ45, 4 SFP GE | 4 GE RJ45 (2 bypass), 4 SFP GE |
| **10G BASE-SR SFP+ Ports** | — | — | — |
| **SSL/TLS Processing** | Software | Software | Hardware |
| **USB Interfaces** | 2 | 2 | 2 |
| **Storage** | 64 GB SSD | 480 GB SSD | 480 GB SSD |
| **Form Factor** | Desktop | 1U | 1U |
| **Trusted Platform Module (TPM)** | — | — | — |
| **Power Supply** | Single | Single | Dual |
| **System Performance** | | | |
| **Throughput** | 100 Mbps | 500 Mbps | 1 Gbps |
| **Latency** | <5ms | <5ms | <5ms |
| **High Availability** | Active/Passive, Active/Active Clustering | Active/Passive, Active/Active Clustering | Active/Passive, Active/Active Clustering |
| **Application Licenses** | Unlimited | Unlimited | Unlimited |
| **Administrative Domains** | — | 32 | 32 |
| All performance values are “up to” and vary depending on the system configuration. | | | |
| **Dimensions** | | | |
| **Height x Width x Length (inches)** | 8.5 × 5.98 × 1.59 | 1.73 × 17.24 × 16.53 | 1.73 × 17.24 × 16.54 |
| **Height x Width x Length (mm)** | 216 × 152 × 40.5 | 44 × 438 × 420 | 44 × 438 × 420 |
| **Weight** | 3.42 lbs (1.55 kg) | 11.91 lbs (5.4 kg) | 14.99 lbs (6.8 kg) |
| **Rack Mountable** | N/A | ✓ | ✓ |
| **Environment** | | | |
| **Power Required** | 100–240V AC, 50–60 Hz | 100–240V AC, 50–60 Hz | 100–240V AC, 50–60 Hz |
| **Maximum Current** | 110V/1.2A, 220V/1.2A | 100V/1.53A, 240V/0.64A | 100V/1.66A, 240V/0.69A |
| **Power Consumption (Average)** | 18 W | 127.33 W | 138.74 W |
| **Heat Dissipation** | 74 BTU/h | 521.38 BTU/h | 568.09 BTU/h |
| **Operating Temperature** | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) |
| **Storage Temperature** | 32°F ~ 104°F (0°C ~ 40°C) | -13°F to 158°F (-25°C to 75°C) | -13°F to 158°F (-25°C to 75°C) |
| **Forced Airflow** | N/A (fanless) | Front to Back | Front to Back |
| **Humidity** | 10% to 85% non-condensing | 5% to 95% non-condensing | 5% to 95% non-condensing |
| **Compliance** | | | |
| **Safety Certifications** | FCC Class A Part 15, RCM, VCCI, CE, UL/cUL, CB | FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL | FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL |

## Specifications

| | FORTIWEB 1000F | FORTIWEB 2000F | FORTIWEB 3000F | FORTIWEB 4000F |
|---|---|---|---|---|
| **Hardware** | | | | |
| **10/100/1000 Interfaces (RJ45 ports)** | 8 bypass,<br>4x SFP GE (non-bypass) | 4GE (4 bypass), 4 SFP GE | 8GE (8 bypass) | 8GE (8 bypass) |
| **10G BASE-SR SFP+ Ports** | 2 | 4 | 10 (2 bypass) | 10 (2 bypass) |
| **40G QSFP** | — | — | — | 2 bypass |
| **SSL/TLS Processing** | Hardware | Hardware | Hardware | Hardware |
| **USB Interfaces** | 2 | 2 | 2 | 2 |
| **Storage** | 2× 480 GB SSD | 2 × 480 GB SSD | 2 × 960 GB SSD | 2 × 960 GB SSD |
| **Form Factor** | 2U | 2U | 2U | 2U |
| **Trusted Platform Module (TPM)** | ✓ | ✓ | ✓ | ✓ |
| **Power Supply** | Dual Hot Swappable | Dual Hot Swappable | Dual Hot Swappable | Dual Hot Swappable |
| **System Performance** | | | | |
| **Throughput** | 2.5 Gbps | 5 Gbps | 10 Gbps | 70 Gbps |
| **Latency** | <5ms | <5ms | <5ms | <5ms |
| **High Availability** | Active/Passive, Active/Active Clustering | Active/Passive, Active/Active Clustering | Active/Passive, Active/Active Clustering | Active/Passive, Active/Active Clustering |
| **Application Licenses** | Unlimited | Unlimited | Unlimited | Unlimited |
| **Administrative Domains** | 64 | 64 | 64 | 64 |
| All performance values are “up to” and vary depending on the system configuration. | | | | |
| **Dimensions** | | | | |
| **Height x Width x Length (inches)** | 3.46 × 16.93 × 19.73 | 3.5 × 17.2 × 20.8 | 3.5 × 17.5 × 22.6 | 3.5 × 17.5 × 22.6 |
| **Height x Width x Length (mm)** | 88 × 430 × 501.20 | 88 × 438 × 530 | 88 × 444 × 574 | 88 × 444 × 574 |
| **Weight** | 28 lbs (12.8 kg) | 33 lbs (15 kg) | 56.2 lbs (22.5 kg) | 56.2 lbs (22.5 kg) |
| **Rack Mountable** | ✓ with flanges | ✓ | ✓ | ✓ |
| **Environment** | | | | |
| **Power Required** | 100–240V AC, 50–60 Hz | 100–240V AC, 60–50 Hz | 100–240V AC, 60–50 Hz | 100–240V AC, 60–50 Hz |
| **Maximum Current** | 100V/5A, 240V/3A | 120V/6A, 240V/3A | 120V/2.6A, 240V/1.3A | 120V/3A, 240V/1.5A |
| **Power Consumption (Average)** | 140 W | 200 W | 200 W | 248.5 W |
| **Heat Dissipation** | 471 BTU/h | 1433 BTU/h | 1045.5 BTU/h | 1219.8 BTU/h |
| **Operating Temperature** | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) |
| **Storage Temperature** | -4°F to 158°F (-20°C to 70°C) | -4°F to 158°F (-20°C to 70°C) | -4°F to 158°F (-20°C to 70°C) | -4°F to 158°F (-20°C to 70°C) |
| **Forced Airflow** | Front to Back | Front to Back | Front to Back | Front to Back |
| **Humidity** | 5% to 90% non-condensing | 5% to 90% non-condensing | 5% to 90% non-condensing | 5% to 90% non-condensing |
| **Compliance** | | | | |
| **Safety Certifications** | FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL | FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL | FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL | FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL |

# Specifications

| VIRTUAL MACHINES | FORTIWEB-VM (1 VCPU) | FORTIWEB-VM (2 VCPU) | FORTIWEB-VM (4 VCPU) | FORTIWEB-VM (8 VCPU) | FORTIWEB-VM (16 VCPU) |
|---|---|---|---|---|---|
| **System Performance** | | | | | |
| **HTTP Throughput** | 25 Mbps | 100 Mbps | 500 Mbps | 3 Gbps | 6 Gbps |
| **Application Licenses** | Unlimited | Unlimited | Unlimited | Unlimited | Unlimited |
| **Administrative Domains** | 4 to 64 based on the amount of memory allocated | | | | |
| **Virtual Machine** | | | | | |
| **Hypervisor Support** | VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Oracle Cloud. Please see FortiWeb VM Installation Guide for versions supported. | | | | |
| **vCPU Support (Minimum / Maximum)** | 1 | 2 | 2 / 4 | 2 / 8 | 2 / 16 |
| **Network Interface Support (Minimum / Maximum)** | 1 / 10 | 1 / 10 | 1 / 10 | 1 / 10 | 1 / 10 |
| **Storage Support (Minimum / Maximum)** | 40 GB / 2 TB | 40 GB / 2 TB | 40 GB / 2 TB | 40 GB / 2 TB | 40 GB / 2 TB |
| **Memory Support (Minimum / Maximum)** | 1024 MB / Unlimited for 64-bit | 1024 MB / Unlimited for 64-bit | 1024 MB / Unlimited for 64-bit | 1024 MB / Unlimited for 64-bit | 1024 MB / Unlimited for 64-bit |
| **Recommended Memory** | 8 GB | 8 GB | 16 GB | 32 GB | 64 GB |
| **High Availability Support** | ✓ | ✓ | ✓ | ✓ | ✓ |

Actual performance values may vary depending on the network traffic and system configuration. Performance metrics were observed using 4 x Intel(R) Xeon(R) Gold 6242 CPU @ 2.80GHz running VMware ESXi 6.7 with 8 GB of vRAM assigned to the 1 vCPU and 2 vCPU FortiWeb Virtual Appliance, 16 GB assigned to the 4 vCPU, 32 GB assigned to the 8 vCPU and 64 GB assigned to the 16 vCPU FortiWeb Virtual Appliance.

| CONTAINER APPLIANCES | FORTIWEB-VMC01 | FORTIWEB-VMC02 | FORTIWEB-VMC04 | FORTIWEB-VMC08 |
|---|---|---|---|---|
| **System Performance** | | | | |
| **HTTP Throughput (Maximum)** | 25 Mbps | 100 Mbps | 500 Mbps | 3 Gbps |
| **Application Licenses** | Unlimited | Unlimited | Unlimited | Unlimited |
| **Administrative Domains** | 4 to 64 based on the amount of memory allocated | | | |
| **Virtual Appliance** | | | | |
| **Container Manager Support** | Docker | | | |
| **Network Interface Support (Minimum / Maximum)** | 1 / 10 | 1 / 10 | 1 / 10 | 1 / 10 |
| **Storage Support (Minimum / Maximum)** | 30 GB / 500 GB | 30 GB / 500 GB | 30 GB / 500 GB | 30 GB / 500 GB |
| **Memory Support (Minimum)** | 4 GB | 4 GB | 4 GB | 4 GB |
| **Recommended Memory** | 8 GB | 8 GB | 8 GB | 8 GB |
| **High Availability Support** | — | — | — | — |

Throughputs and other metrics are maximum values permitted for each version. Actual performance values may vary depending on the network traffic and system configuration.

## Ordering Information

| Product | SKU | Description |
|---|---|---|
| **FortiWeb 100F** | FWB-100F | Web Application Firewall — 4x GE RJ45 ports, 4 GB RAM, 1× 64 GB SSD storage. |
| **FortiWeb 400F** | FWB-400F | Web Application Firewall — 4x GE RJ45 ports, 4x GE SFP ports, 480 GB SSD storage. |
| **FortiWeb 600F** | FWB-600F | Web Application Firewall — 4x GE RJ45 (2 bypass), 4x GE SFP ports, 480 GB SSD storage. |
| **FortiWeb 1000F** | FWB-1000F | Web Application Firewall — 2× 10 GE SFP+ ports, 8x GE RJ45 bypass ports, 4x GE SFP ports, 2x GE management ports, dual AC power supplies, 2× 480 GB SSD storage. |
| **FortiWeb 2000F** | FWB-2000F | Web Application Firewall — 4× 10 GE SFP+ ports, 4x GE RJ45 bypass ports, 4x GE SFP ports, 2x GE management ports, dual AC power supplies, 2× 480 GB SSD storage. |
| **FortiWeb 3000F** | FWB-3000F | Web Application Firewall — 10× 10 GE SFP+ ports (2 bypass), 8x GE RJ45 bypass ports, 2x GE management ports, dual AC power supplies, 2× 960 GB SSD storage. |
| **FortiWeb 4000F** | FWB-4000F | Web Application Firewall — 2× 40 GE bypass ports, 10× 10 GE SFP+ ports (2 bypass), 8x GE RJ45 bypass ports, 2x GE management ports, dual AC power supplies, 2× 960 GB SSD storage. |
| **FortiWeb-VM01** | FWB-VM01 | FortiWeb-VM, up to 1 vCPU supported. 64-bit OS. |
| **FortiWeb-VM02** | FWB-VM02 | FortiWeb-VM, up to 2 vCPUs supported. 64-bit OS. |
| **FortiWeb-VM04** | FWB-VM04 | FortiWeb-VM, up to 4 vCPUs supported. 64-bit OS. |
| **FortiWeb-VM08** | FWB-VM08 | FortiWeb-VM, up to 8 vCPUs supported. 64-bit OS. |
| **FortiWeb-VM16** | FWB-VM16 | FortiWeb-VM, up to 16 vCPUs supported. 64-bit OS. |
| **FortiWeb-VMC01** | FWB-VMC01 | FWB-VMC01 for container-based environments. Up to 25 Mbps throughput. |
| **FortiWeb-VMC02** | FWB-VMC02 | FWB-VMC02 for container-based environments. Up to 100 Mbps throughput. |
| **FortiWeb-VMC04** | FWB-VMC04 | FWB-VMC04 for container-based environments. Up to 500 Mbps throughput. |
| **FortiWeb-VMC08** | FWB-VMC08 | FWB-VMC08 for container-based environments. Up to 2 Gbps throughput. |
| **Central Manager 10** | FWB-CM-BASE | FortiWeb Central Manager license key, manage up to 10 FortiWeb devices, VMware vSphere. |
| **Central Manager Unlimited** | FWB-CM-UL | FortiWeb Central Manager license key, manage unlimited number of FortiWeb devices, VMware vSphere. |
| **Optional Accessories** | **SKU** | **Description** |
| **AC Power Supply** | SP-FWB600F-PS | AC power supply for FWB-600F and FAD-420F, power cable SP-FGPCOR-XX sold separately. |
| | SP-FWB3000F-PS | AC power supply for FWB-3000F and FWB-4000F, power cable SP-FGPCOR-XX sold separately. |
| | SP-FAD400F-PS | AC power supply for FAD-400F, FAZ-300G, FMG-200G, FWB-600E and FPX-400G, module only power cable SP-FGPCOR-XX sold separately. |

The following SKUs adopt the annual subscription licensing scheme:

| Product | SKU | Description |
|---|---|---|
| **FortiWeb-VM01-S Standard** | FC1-10-WBVMS-916-02-DD | Subscription license for FortiWeb-VM (1 CPU) with Standard bundle included. |
| **FortiWeb-VM01-S Advanced** | FC1-10-WBVMS-582-02-DD | Subscription license for FortiWeb-VM (1 CPU) with Advanced bundle included. |
| **FortiWeb-VM01-S Enterprise** | FC1-10-WBVMS-1267-02-DD | Subscription license for FortiWeb-VM (1 CPU) with Enterprise bundle included. |
| **FortiWeb-VM02-S Standard** | FC2-10-WBVMS-916-02-DD | Subscription license for FortiWeb-VM (2 CPU) with Standard bundle included. |
| **FortiWeb-VM02-S Advanced** | FC2-10-WBVMS-582-02-DD | Subscription license for FortiWeb-VM (2 CPU) with Advanced bundle included. |
| **FortiWeb-VM01-S Enterprise** | FC2-10-WBVMS-1267-02-DD | Subscription license for FortiWeb-VM (2 CPU) with Enterprise bundle included. |
| **FortiWeb-VM04-S Standard** | FC3-10-WBVMS-916-02-DD | Subscription license for FortiWeb-VM (4 CPU) with Standard bundle included. |
| **FortiWeb-VM04-S Advanced** | FC3-10-WBVMS-582-02-DD | Subscription license for FortiWeb-VM (4 CPU) with Advanced bundle included. |
| **FortiWeb-VM01-S Enterprise** | FC3-10-WBVMS-1267-02-DD | Subscription license for FortiWeb-VM (4 CPU) with Enterprise bundle included. |
| **FortiWeb-VM08-S Standard** | FC4-10-WBVMS-916-02-DD | Subscription license for FortiWeb-VM (8 CPU) with Standard bundle included. |
| **FortiWeb-VM08-S Advanced** | FC4-10-WBVMS-582-02-DD | Subscription license for FortiWeb-VM (8 CPU) with Advanced bundle included. |
| **FortiWeb-VM01-S Enterprise** | FC4-10-WBVMS-1267-02-DD | Subscription license for FortiWeb-VM (8 CPU) with Enterprise bundle included. |
| **FortiWeb-VM16-S Standard** | FC5-10-WBVMS-916-02-DD | Subscription license for FortiWeb-VM (16 CPU) with Standard bundle included. |
| **FortiWeb-VM16-S Advanced** | FC5-10-WBVMS-582-02-DD | Subscription license for FortiWeb-VM (16 CPU) with Advanced bundle included. |
| **FortiWeb-VM01-S Enterprise** | FC5-10-WBVMS-1267-02-DD | Subscription license for FortiWeb-VM (16 CPU) with Enterprise bundle included. |

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

### FortiCare Services

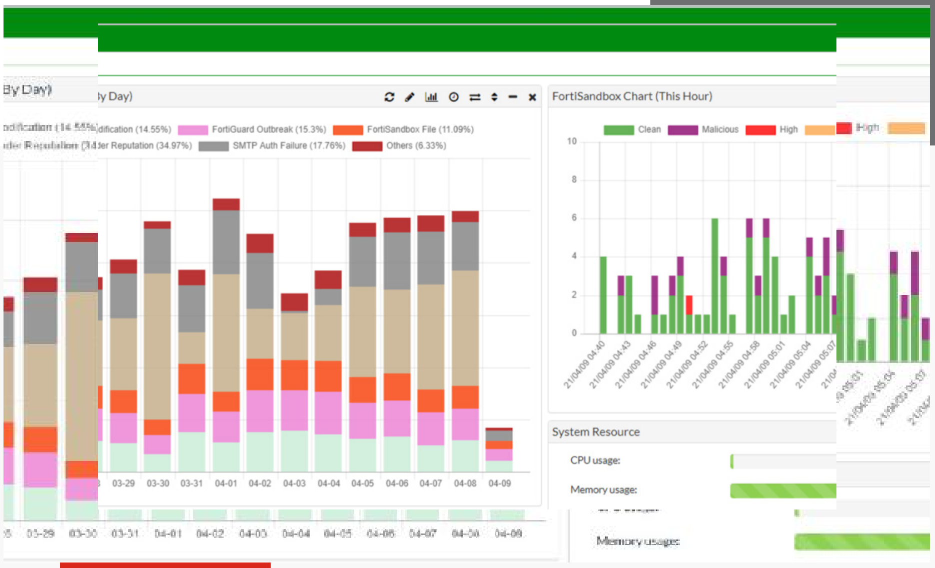
Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution.  Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services.  Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs.  In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

FORTINET

www.fortinet.com

August 8, 2025

# FortiMail™ For Email Security



## Highlights

- Protection against email-borne threats
- Validated performance
- Fabric-enabled email security
- Powered by FortiGuard Labs

## Powerful, Scalable Email Security Protection Available in an Array of Deployment Models

With best-in-class performance validated by independent testing firms, FortiMail delivers advanced multi-layered protection against the full spectrum of email-borne threats. Powered by FortiGuard Labs threat intelligence and integrated into the Fortinet Security Fabric, FortiMail helps your organization prevent, detect, and respond to email-based threats including spam, phishing, malware, zero-day threats, impersonation, and Business Email Compromise (BEC) attacks.

## Features

### Protection Against Email-borne Threats

Powerful anti-spam and anti-malware are complemented by advanced techniques like outbreak protection, content disarm and reconstruction, sandbox analysis, impersonation detection, and other technologies to stop unwanted bulk email, phishing, ransomware, business email compromise, and targeted attacks.

### Validated Performance

Fortinet is one of the only email security vendors to consistently prove the efficacy of FortiMail through independent testing. FortiMail earned a 99.99% Spam Catch Rate from Virus Bulletin.

### Fabric-enabled Email Security

FortiMail is integrated with Fortinet products as well as third-party components help you adopt a proactive approach to security by sharing IoCs across a seamless Security Fabric. It also enables advanced and complementary email security protection for Microsoft 365 and Google Gsuite Cloud email through API-level integration.

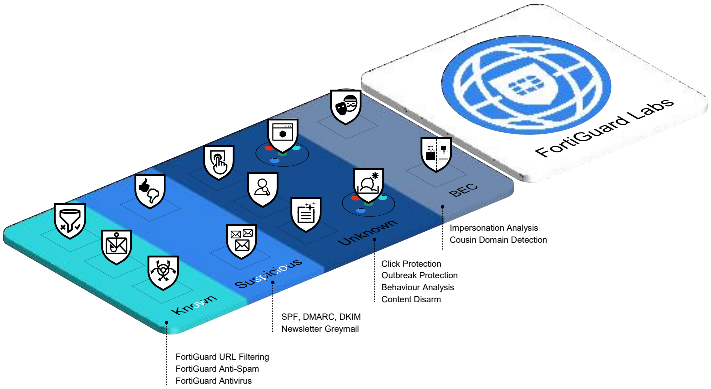
### Powered by FortiGuard Labs

Fortinet FortiMail is powered by threat intelligence and FortiGuard AI-powered Security Services like antivirus, virus outbreak protection, and antispam, from FortiGuard Labs. With visibility across 600,000 customer environments worldwide, FortiGuard Labs is one of the preeminent threat research teams in existence.

## Features

### Proactive Email Security

FortiMail addresses the full spectrum of risks that email poses to organizations, fortified by FortiGuard Labs' global visibility and intelligence on the latest threats.



### Multi-Layered Anti-Spam

Multiple sender, protocol and content inspection techniques shield users from spam and junk mail. Using a combination of reputation analysis, connection filtering, authentication and recipient verification methods allows for fast and accurate email protection. Checks include IP, domain, sender, SPF, DKIM, DMARC and geographical restrictions.

Finally, message structure and content are analyzed based on the digital signature, keywords in context, image analysis, embedded URIs, and more advanced techniques such as behavior analysis and spam outbreak protection. Working together, these techniques consistently identify and block a verified 99.99% of spam in real-world conditions.

### Powerful Anti-Malware

Combining multiple static and dynamic technologies that include signature, heuristic, and behavioral techniques along with virus outbreak prevention, FortiMail protects against a wide range of constantly evolving threats.

### Advanced Threat Protection (ATP)

For an even stronger defense against the very latest threat classes like business email compromise and targeted attacks, FortiMail offers optional content disarm and reconstruction, sandbox analysis, sophisticated spoof detection, and more.

### Integrated Data Loss Prevention

A robust set of capabilities for data loss prevention and email encryption safely deliver sensitive emails and protect against the inadvertent loss of data. These features facilitate compliance with corporate policies and industry regulations.

### Intuitive Controls

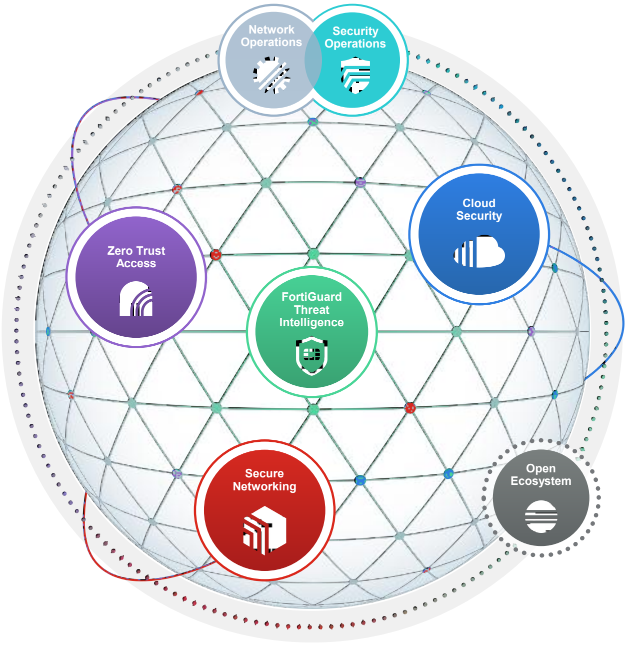
Real-time dashboards, rich reporting, centralized quarantine and simple to use end-user controls allow organizations to get running and realize value quickly.  An intuitive user interface combined with flexible MTA and mail-handling capabilities give full visibility and control over email traffic.

## Features

### Integration with the Fortinet Security Fabric

The future of email security is platform- or fabric-enabled to counter the growing sophistication of threats and multi-vector campaigns. As part of the Fortinet Security Fabric, Indicators of Compromise and other telemetry can be shared for enhanced security across your entire security infrastructure.

IT and security teams are able to more completely connect the dots to identify multi-vector campaigns by sophisticated actors. In addition, intensive and repetitive workflows including response can be automated to reduce the burden on security operations teams.



### Industry Recognized, Top-Rated Performance

FortiMail delivers superior performance as measured by independent third-party testers.

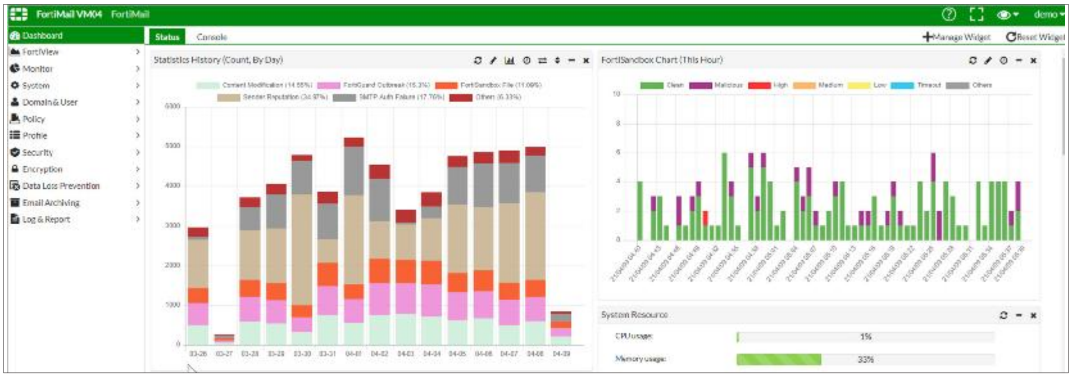
99.99%
Spam Catch Rate

100%
Malware Detected

# Features

### Intuitive Email Management

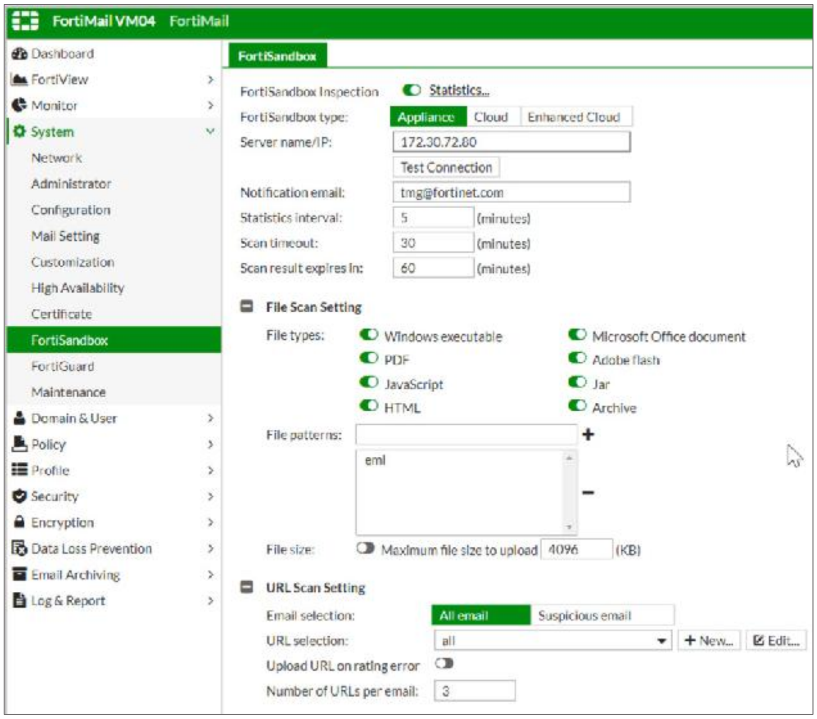
Real-time dashboards, rich reporting, centralized quarantines, and end user controls along with full MTA and mail-handling capabilities provide organizations full visibility and easy control over email traffic.



---

### Easy-to-Use Configuration

Easy-to-use configuration controls make setting up and managing email security – even advanced security capabilities - easy for organizations of all sizes and use cases



FortiSandbox Inspection: Statistics...

FortiSandbox type: Appliance | Cloud | Enhanced Cloud

Server name/IP: 172.30.72.80

Notification email: tmg@fortinet.com

Statistics interval: 5 (minutes)

Scan timeout: 30 (minutes)

Scan result expires in: 60 (minutes)

File Scan Setting

File types: Windows executable, Microsoft Office document, PDF, Adobe flash, JavaScript, Jar, HTML, Archive

File patterns: eml

File size: Maximum file size to upload 4096 (KB)

URL Scan Setting

Email selection: All email | Suspicious email

URL selection: all

Upload URL on rating error

Number of URLs per email: 3

## Hands on or hands off?

## Which FortiMail solution is best for you?

**We want full control.**

Virtual Machines and appliances for teams who want total control over their infrastructure and email security.

**Manage it for us.**

Email security as a service for teams who just want to focus on monitoring and responding to email threats. Fortinet handles the infrastructure.

**Read the FortiMail Cloud data sheet >**

# Features

### High Performance, Flexible Deployment

Scale easily to handle millions of messages per hour. Serving organizations of all sizes, Fortinet provides a wide range of deployment models and operation modes to best match your organization's email security needs.

## Deployment Models

### Appliances and Virtual Machines

FortiMail appliances and virtual machines are for organizations that prefer full control and management over their email security infrastructure for on-premise and cloud use cases.

- Appliances for on-premise environments
- Virtual machines for running on:
  - Popular hypervisor platforms including:
    - VMWare
    - Citrix XenServer
    - Hyper-V
    - KVM
  - Major cloud platforms:
    - AWS
    - Azure
    - Google Cloud
    - Oracle
    - AliCloud

### FortiMail Cloud

FortiMail Cloud for organizations that want simple, easy-to-use email security as-a-service for both on-premise and cloud-based email services.

## Operation Modes

### Gateway Mode

Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for analysis. FortiMail then relays safe email to its destination email server for delivery.

### Microsoft and Google Cloud Email API Integration

FortiMail can be deployed out of line to simplify deployment, so no MX record change is required, and leverage the native Microsoft and Google APIs to deliver threat detection and post-delivery message clawback. Broad flexibility is possible with clawback to create policies that address compliance or unique business requirements, such as building search parameters based on keywords, file name, or content type. These capabilities can serve as powerful complements to native Microsoft and Google security features to bolster overall efficacy and reduce risk.

### Transparent Mode

Transparent mode eliminates the need to change the DNS MX record, or to change the existing email server network configuration. Transparent mode is particularly appealing for service providers that want to extend email security services to their customer bases. Not available with FortiMail Cloud.

### Server Mode

The FortiMail device acts as a standalone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP, and WebMail access.

## Feature Bundles

We want full control.

| Feature | Base Bundle | Enterprise Advanced Threat Protection Bundle | Ent. ATP with Cloud Email API Support Bundle |
|---|---|---|---|
| 99.99% Spam Capture Rate | ✓ | ✓ | ✓ |
| Advanced Multi-Layer Malware Detection | ✓ | ✓ | ✓ |
| Inbound and Outbound Filtering | ✓ | ✓ | ✓ |
| Integration with Customer LDAP | ✓ | ✓ | ✓ |
| Secure Message Delivery (TLS) | ✓ | ✓ | ✓ |
| Message Tracking | ✓ | ✓ | ✓ |
| Virus Outbreak Service | ✓ | ✓ | ✓ |
| Identity-Based Encryption (IBE) | ✓ | ✓ | ✓ |
| Reporting | ✓ | ✓ | ✓ |
| Email Data Loss Prevention | ✓ | ✓ | ✓ |
| Content Disarm and Reconstruction |  | ✓ | ✓ |
| URL Click Protection |  | ✓ | ✓ |
| Impersonation Analysis |  | ✓ | ✓ |
| Cloud Sandboxing |  | ✓ | ✓ |
| Real-time Scanning of Microsoft and Google Mailboxes |  |  | ✓ |
| Scheduled Scanning of Microsoft and Google Mailboxes |  |  | ✓ |
| Post-delivery Clawback of Newly Discovered Email Threats |  |  | ✓ |

## Additional Add-on Capabilities

### Email Continuity

Email Continuity for FortiMail Cloud is designed to protect valuable productivity by providing emergency mailbox services when organizations experience an outage of their email services.

### Dynamic Image Analysis Service

Protects your organization and employees against inappropriate and sexually explicit images.

## Integrations with Fortinet Solutions

FortiAnalyzer

FortiIsolator

FortiSandbox Cloud

FortiSOAR

FortiAnalyzer Cloud

FortiNDR

FortiSIEM

# Features Summary

### SYSTEM

Wide range of deployment and operation options
– On-premise or public or private cloud deployment
– Gateway, Microsoft and Google API connectors, Transparent, and Server Mode

Inbound and Outbound Inspection

Support for multiple email domains with per-domain customization
– MSSP multi-tenant support with white label support
– Multi-tier administration

IPv4 and IPv6 Address Support

Virtual Hosting using Source and/or Destination IP Address Pools

SMTP Authentication Support via LDAP, RADIUS, POP3 and IMAP

LDAP-Based Email Routing

Per User Inspection using LDAP Attributes on a Per Policy (Domain) Basis

Geographic IP location-based policy

Comprehensive Webmail Interface for Server Mode Deployments and Quarantine Management

Mail Queue Management

Multiple Language Support for Webmail and Admin Interface

SMTP RFC Compliance

Modern HTML 5 GUI

Independently tested by SELabs, and Virus Bulletin

Compatibility with cloud services e.g. Microsoft 365, Google Workspace, Amazon AWS, and Microsoft Azure

DNS-based Authentication of Named Entities (DANE) support

### ANTISPAM

FortiGuard Antispam Service
– Sender and domain reputation
– Spam and attachment signatures
– Dynamic heuristic rules
– Outbreak protection

Full FortiGuard URL Category Filtering includes
– Spam, malware and phishing URLs
– Pornographic and adult URLs
– Newly registered domains

Greylisting for IPv4, IPv6 addresses and email accounts

Local sender reputation (IPv4, IPv6 and End Point ID-based)

Behavioral analysis

Integration with third-party spam URI and real-time blacklists (SURBL/RBL)

Newsletter (greymail) and suspicious newsletter detection

PDF Scanning and image analysis

Block/safe lists at global, domain, and user levels

Support for enterprise sender identity standards
– Sender Policy Framework (SPF)
– Domain Keys Identified Mail (DKIM)
– Domain-Based Message Authentication (DMARC)

Flexible action and notification profiles

Multiple system and per-user self-service quarantines

### TARGETED ATTACK PROTECTION

Content Disarm and Reconstruction
– Neutralize Office and PDF documents (remove macros, active content, attachments, and more)
– Neutralize email HTML content by removing hyperlinks / rewrite URLs

Business Email Compromise (BEC)
– Multi-level anti-spoof protection
– Impersonation analysis — manual and automatic address impersonation detection
– Cousin domain detection

URL Click Protect to rewrite URLs and rescan on access

Integration with FortiIsolator Browser Isolation platform to neutralize browser-based threats

### API INTEGRATION

Microsoft 365 and Google Gsuite Email Integration
– Post-delivery threat clawback
– Scheduled scan
– Real-time scanning
– Internal mail scanning

### CONTENT DETECTION

FortiGuard Antivirus Service detection
– CPRL signature checking
– Heuristic based behavioral detection
– Greyware detection

FortiGuard Virus Outbreak Protection Service
– Global threat intelligence and data analytics

Active content detection (PDF & Office Documents)

Rescan for threats on quarantine release

Custom file hash checking

Mime and file type detection

Comprehensive data-loss prevention with file fingerprinting and sensitive data detection
– Automatic Windows fileshare and manual upload file fingerprinting
– Healthcare, Finance, personally identifiable information and profanity detection

Automatic decryption of Archives, PDF and Office Documents using built-in and administrator-defined password lists and word detection within email body

PDF Scanning and image analysis

Dynamic Image Analysis Service
– Identify and report on illicit and sexually explicit content

### ENCRYPTION

Comprehensive encryption support
– Server to server TLS with granular ciphersuite control and optional enforcement
– S/MIME
– Clientless encryption to the recipient desktop using Identity Based Encryption (IBE)
– Optional Outlook plugin to trigger Identity Based Encryption (IBE)

### MANAGEMENT, LOGGING, AND REPORTING

Basic/advanced management modes

Per domain, role-based administration accounts

Comprehensive activity, configurations change and incident logging and reporting

Built-in reporting module

Detailed message tracking

Centralized quarantine for large scale deployments

Optional centralized logging and reporting with FortiAnalyzer

SNMP support using standard and private MIB with threshold-based traps

Local or external storage server support, including iSCSI devices

External Syslog support

Open REST API for configuration and management

### HIGH AVAILABILITY (HA)

High availability supported in all deployment scenarios
– Active-Passive mode
– Active-Active configuration synchronization mode

Quarantine and mail queue synchronization

Device failure detection and notification

Link status, failover and redundant interface support

### ADVANCED

Policy-based e-mail archiving with remote storage options
– Support for Exchange journal archiving

Advanced Email Server feature set including
– Comprehensive webmail interface
– POP3, IMAP mail access
– Calendaring functions
– Undo Send

SAML 2.0 SSO and ADFS integration for webmail and quarantine access

### SUPPORT

Simple support options with inclusive bundles

Advanced RMA Support

Professional services and installation support options

## Specifications

| | FORTIMAIL 200F | FortiMail 400F | FortiMail 900F | FortiMail 900G |
|---|---|---|---|---|
| **Recommended Deployment Scenarios** | | | | |
| | Small businesses, branch offices, and organizations | Small to midsized organizations | Mid to large enterprise, education, and government departments | Mid to large enterprise, education, and government departments |
| **Hardware Specifications** | | | | |
| **10/100/1000 Interfaces (Copper, RJ45)** | 4 | 4 | 4 | 4 |
| **SFP Gigabit Ethernet Interface** | — | — | 2 | 2 |
| **SFP+ 10 Gigabit Ethernet Interface** | — | — | — | — |
| **Redundant Hot Swappable Power Supplies** | — | — | ✓ | ✓ |
| **Storage** | 1× 1TB | 2× 1 TB | 2× 2 TB (2× 2 TB Optional) | 2× 4 TB (2× 4 TB Optional) |
| **Secure Encrypted Drives (SED)** | — | — | — | ✓ |
| **RAID Storage Management** | — | Software 0, 1 | Hardware 0, 1, 5, 10, Hot Spare (Based on Drive Count) | Hardware 0, 1, 5, 10, Hot Spare (Based on Drive Count) |
| **Memory** | 4 GB | 8 GB | 16 GB | 16 GB |
| **Form Factor** | Rack Mount, 1U | Rack Mount, 1U | Rack Mount, 1U | Rack Mount, 1U |
| **Trusted Platform Module (TPM)** | ✓ | ✓ | ✓ | ✓ |
| **Power Supply** | Single | Single (Dual Optional) | Dual | Dual |
| **System Specifications** | | | | |
| **Protected Email Domains*** | 20 | 70 | 500 | 500 |
| **Recipient-based Policies (per Domain / per System) — Incoming or Outgoing** | 60 / 300 | 400 / 1500 | 600 / 2000 | 600 / 2000 |
| **Server Mode local mailboxes** | 150 | 400 | 1500 | 1500 |
| **Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)** | 50 / 60 | 50 / 200 | 50 / 400 | 50 / 400 |
| **Data Loss Prevention** | — | ✓ | ✓ | ✓ |
| **Centralized Quarantine** | — | ✓ | ✓ | ✓ |
| **Microsoft 365 and Google Gsuite Email API Integration** | — | Optional | Optional | Optional |
| **Performance (Messages/Hour) [Without queuing based on 100 KB message size]** | | | | |
| **Email Routing (per hour)**** | 50 K | 250 K | 800 K | 1.3 million |
| **FortiGuard Antispam + Virus Outbreak (per hour)**** | 40 K | 200 K | 500 K | 900 K |
| **FortiGuard Enterprise ATP (per hour)**** | 30 K | 150 K | 400 K | 650 K |
| **Cloud API Performance (Messages/Hour) [Without queuing based on 100 KB message size]** | | | | |
| **Email Routing (per hour)**** | 18 K | 83 K | 241 K | 320 K |
| **FortiGuard Antispam + Virus Outbreak (per hour)**** | 14 K | 72 K | 170 K | 235 K |
| **FortiGuard Enterprise ATP (per hour)**** | 12 K | 58 K | 148 K | 200 K |
| **Dimensions** | | | | |
| **Height x Width x Length (inches)** | 1.73 × 17.24 × 16.61 | 1.73 × 17.24 × 16.38 | 1.75 × 17.00 × 27.61 | 1.7 × 17.2 × 24 |
| **Height x Width x Length (mm)** | 44 × 438 × 422 | 44 × 438 × 416 | 44 × 438 × 701 | 44 × 438 × 610 |
| **Weight** | 11.9 lbs (5.4 kg) | 25.0 lbs (11.0kg) | 33.1 lbs (15.00 kg) | 28.37 lbs (12.87 kg) |
| **Environment** | | | | |
| **Power Source** | 100–240V AC, 50–60 Hz | 100–240V AC, 50–60 Hz | 100–240V AC, 50–60 Hz | 100–240V AC, 50–60 Hz |
| **Maximum Current** | 100V / 3A, 240V / 1.5A | 100V / 5A, 240V / 3A | 100V / 5A, 240V / 2.5A | 6A / 100V, 3A / 240V |
| **Maximum Power Required** | 62 W | 113 W | 190 W | 189.4 W |
| **Power Consumption (Average)** | 51 W | 77 W | 174 W | 165.56 W |
| **Heat Dissipation** | 245 BTU/h | 418 BTU/h | 681 BTU/h | 646.23 BTU/h |
| **Forced Airflow** | Front to back | Front to back | Front to back | Front to back |
| **Humidity** | 5% to 90% non-condensing | 5% to 90% non-condensing | 5% to 90% non-condensing | 5% to 93% non-condensing |
| **Operating Temperature** | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) | 50°F to 95°F (10°C to 35°C) |
| **Storage Temperature** | -4°F to 158°F (-20°C to 70°C) | -4°F to 158°F (-20°C to 70°C) | -4°F to 158°F (-20°C to 70°C) | -40°F to 158°F (-40°C to 70°C) |
| **Compliance** | | | | |
| | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, RoHS | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS |
| **Certification** | | | | |
| | VBSpam and VB100 rated. Common Criteria evaluation in process (NIAP). NIST CMVP Implementation under test (FIPS140-3). | | | |

* Protected Email Domains is the total number of email domains that can be configured on the appliance.
Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.
Advanced management license increases the protected domain limit by 50%.

** Tested using FortiMail 7.0

# Specifications

| | FORTIMAIL 2000F | FORTIMAIL 3000F | FORTIMAIL 3000FH |
|---|---|---|---|
| **Recommended Deployment Scenarios** | | | |
| | Large enterprise, education, and government departments | Highest performing appliance for the largest corporate, university, ISP, and carriers | Highest performing appliance for the largest corporate, ISP, and carriers requiring more memory |
| **Hardware Specifications** | | | |
| **10/100/1000 Interfaces (Copper, RJ45)** | 4 | 4 | 4 |
| **SFP Gigabit Ethernet Interface** | 2 | 2 | 2 |
| **SFP+ 10 Gigabit Ethernet Interface** | — | 2 | 2 |
| **Redundant Hot Swappable Power Supplies** | ✓ | ✓ | ✓ |
| **Storage** | 2× 2 TB SAS (6× 2 TB Optional) | 2× 2 TB (10× 2 TB Optional) | 2× 2 TB (10× 2 TB Optional) |
| **Secure Encrypted Drives (SED)** | — | — | — |
| **RAID Storage Management** | Hardware; 1, 5, 10, 50, Hot Spare (Based on drive count) | Hardware; 1, 5, 10, 50, Hot Spare (Based on drive count) | Hardware; 1, 5, 10, 50, Hot Spare (Based on drive count) |
| **Memory** | 32 GB | 64 GB | 512 GB |
| **Form Factor** | Rack Mount, 2U | Rack Mount, 2U | Rack Mount, 2U |
| **Trusted Platform Module (TPM)** | ✓ | ✓ | ✓ |
| **Power Supply** | Dual | Dual | Dual |
| **System Specification** | | | |
| **Protected Email Domains*** | 1000 | 2000 | 2000 |
| **Recipient-Based Policies (per Domain / per System) — Incoming or Outgoing** | 800 / 3000 | 1500 / 7500 | 1500 / 7500 |
| **Server Mode local mailboxes** | 2000 | 3000 | 3000 |
| **Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)** | 50 / 400 | 50 / 600 | 50 / 600 |
| **Data Loss Prevention** | ✓ | ✓ | ✓ |
| **Centralized Quarantine** | ✓ | ✓ | ✓ |
| **Microsoft 365 and Google Gsuite Email API Integration** | Optional | Optional | Optional |
| **Performance (Messages/Hour) [Without queuing based on 100 KB message size]** | | | |
| **Email Routing (per hour)**** | 1.6 Million | 3.5 Million | 3.5 Million |
| **FortiGuard Antispam + Virus Outbreak (per hour)**** | 1.1 Million | 2.6 Million | 2.6 Million |
| **FortiGuard Enterprise ATP (per hour)**** | 800 K | 2.1 Million | 2.1 Million |
| **Cloud API Performance (Messages/Hour) [Without queuing based on 100 KB message size]** | | | |
| **Email Routing (per hour)**** | 372 K | 705 K | 705 K |
| **FortiGuard Antispam + Virus Outbreak (per hour)**** | 280 K | 560 K | 560 K |
| **FortiGuard Enterprise ATP (per hour)**** | 233 K | 465 K | 465 K |
| **Dimensions** | | | |
| **Height x Width x Length (inches)** | 3.5 × 17.2 × 25.5 | 3.5 × 17.2 × 25.5 | 3.5 × 17.2 × 25.5 |
| **Height x Width x Length (mm)** | 89 × 437 × 647 | 88 × 440 × 745 | 88 × 440 × 745 |
| **Weight** | 32 lbs (14.5 kg) | 55.8 lbs (25.3 kg) | 55.8 lbs (25.3 kg) |
| **Environment** | | | |
| **Power Source** | 100–240V AC, 50–60 Hz | 100-240 VAC, 60-50 Hz | 100-240 VAC, 60-50 Hz |
| **Maximum Current** | 10.0A / 110V, 3.5A / 240V | 9.8A / 110V, 4.9A / 220V | 9.8A / 110V, 4.9A / 220V |
| **Maximum Power Required** | 219 W | 592.9 W | 592.9 W |
| **Power Consumption (Average)** | 189 W | 485.1 W | 485.1 W |
| **Heat Dissipation** | 781 BTU/h | 1325 BTU/h | 1325 BTU/h |
| **Forced Airflow** | Front to back | Front to back | Front to back |
| **Humidity** | 8% to 90% non-condensing | 8% to 90% non-condensing | 8% to 90% non-condensing |
| **Operating Temperature** | 41°F to 95°F (5°C to 35°C) | 50°F to 95°F (10°C to 35°C) | 50°F to 95°F (10°C to 35°C) |
| **Storage Temperature** | -40°F to 140°F (-40°C to 60°C) | -40°F to 158°F (-40°C to 70°C) | -40°F to 158°F (-40°C to 70°C) |
| **Compliance** | | | |
| | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS |
| **Certification** | | | |
| | VBSpam and VB100 rated. Common Criteria evaluation in process (NIAP). NIST CMVP Implementation under test (FIPS140-3). | | |

* Protected Email Domains is the total number of email domains that can be configured on the appliance. Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned. Advanced management license increases the protected domain limit by 50%.

** Tested using FortiMail 7.0

# Specifications

| Technical Specifications for FortiMail Virtual Appliances | VM01 | VM02 | VM04 | VM08 | VM16 | VM32 |
|---|---|---|---|---|---|---|
| **Recommended Deployment Scenarios *** | | | | | | |
| | Small businesses, branch offices, and organizations | Small to midsized organizations | Mid to large enterprise | Large enterprise | Large enterprise | Large enterprise |
| **Technical Specifications** | | | | | | |
| **Hypervisors Supported** | VMWare ESX/ESXi 6.0 and later, Citrix XenServer v5.6 SP2/6.0 and later, Microsoft Hyper-V Server 2008 R2/2012/2012 R2/2016/2019, KVM qemu 2.12.1 and later, AWS (Amazon Web Services), Nutanix AHV**, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure*** | | | | | |
| **Maximum Virtual CPUs Supported** | 1 | 2 | 4 | 8 | 16 | 32 |
| **Virtual NICs Required (Minimum/Maximum)** | 1 / 4 | 1 / 4 | 1 / 6 | 1 / 6 | 1 / 6 | 1 / 6 |
| **Virtual Machine Storage Required (Minimum/Maximum) ****** | 250 GB / 1 TB | 250 GB / 2 TB | 250 GB / 4 TB | 250 GB / 8 TB | 250 GB / 12 TB | 250 GB / 24 TB |
| **Virtual Machine Memory Required (Minimum/Maximum)** | 2 GB / 4 GB | 2 GB / 8 GB | 4 GB / 16 GB | 4 GB / 64 GB | 4 GB / 128 GB | 4 GB / 128 GB |
| **Performance (Messages/Hour) [Without queuing based on 100 KB message size] ******* | | | | | | |
| **Email Routing (per hour) **** | 34 K | 67 K | 306 K | 675 K | 875 K | 1.2 M |
| **FortiGuard Antispam + Virus Outbreak (per hour) **** | 30 K | 54 K | 279 K | 630 K | 817 K | 1.1 M |
| **FortiGuard Enterprise ATP (per hour) **** | 26 K | 52 K | 225 K | 585 K | 758 K | 1.0 M |
| **Cloud API Performance (Messages/Hour) [Without queuing based on 100 KB message size] ******* | | | | | | |
| **Email Routing (per hour) **** | N/A | 23 K | 110 K | 295 K | 495 K | 940 K |
| **FortiGuard Antispam + Virus Outbreak (per hour) **** | N/A | 18 K | 96 K | 226 K | 383 K | 740 K |
| **FortiGuard Enterprise ATP (per hour) **** | N/A | 16 K | 75 K | 197 K | 311 K | 620 K |
| **System Specifications** | | | | | | |
| **Protected Email Domains ********* | 20 | 70 | 500 | 1000 | 1500 | 2000 |
| **Recipient-Based Policies (Domain / System) — Incoming or Outgoing** | 60 /300 | 400 / 1500 | 800 / 3000 | 800 / 3000 | 1500 / 7500 | 1500 / 7500 |
| **Server Mode local mailboxes** | 150 | 400 | 1500 | 2000 | 3000 | 3000 |
| **Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)** | 50 / 60 | 50 / 200 | 50 / 400 | 50 / 400 | 50 / 600 | 50 / 600 |
| **Data Loss Prevention** | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Centralized Quarantine** | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Microsoft 365 and Google Gsuite Email API Integration** | — | Optional | Optional | Optional | Optional | Optional |
| **Certification** | | | | | | |
| | VBSpam and VB100 rated. Common Criteria evaluation in process (NIAP). NIST CMVP Implementation under test (FIPS140-3). | | | | | |

| | |
|---|---|
| * | Recommended sizing for Gateway and Transparent deployments. For Server Mode, see Server Mode Mailbox metric.<br>If unsure, please validate the model selection by checking the peak mail flow rates and average message size detail with a FortiMail specialist. |
| ** | FortiMail 7.0.1 has been validated on Nutanix AHV 20201105.2096 and AOS 5.20.1.1. |
| *** | Transparent mode deployment is not fully supported on Microsoft HyperV and cloud hypervisors due to limitations in the available network configurations. |
| **** | For the initial VM setup, 250GB is required to install the default Fortinet OVF file. After deployment, the default OVF file can be deleted and the disk space set no less than 50 GB. |
| ***** | Hardware dependent. Indicative figures based on a VMWare 6.0 system utilizing 2x Intel Xeon E5-2620 v4 @ 2.10 GHz restricted to the specified number of cores. |
| ****** | Protected Email Domains is the total number of email domains that can be configured on the appliance.<br>Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.<br>Advanced management license increases the protected domain limit by 50%. |

# Order Information

For information on ordering, please talk with your Fortinet account manager, or refer to the Ordering Guide for a full list of FortiMail-related SKUs and pricing information.

| FortiMail Product | SKU | Description |
|---|---|---|
| **FortiMail 200F** | FML-200F | Email Security Appliance — 4x GE RJ45 ports, 1 TB storage |
| **FortiMail 400F** | FML-400F | Email Security Appliance — 4x GE RJ45 ports, 2 TB storage |
| **FortiMail 900F** | FML-900F | Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage |
| **FortiMail 900G** | FML-900G | Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 8 TB default storage |
| **FortiMail 2000F** | FML-2000F | Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage |
| **FortiMail 3000F** | FML-3000F | Email Security Appliance — 4x GE RJ45 ports, 2× 10 GE SFP+ slots, 2x GE SFP slots, dual AC power supplies, 4 TB default storage |
| **FortiMail VM** | | |
| **FortiMail VM01** | FML-VM01 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 1x vCPU core |
| **FortiMail VM02** | FML-VM02 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 2x vCPU cores |
| **FortiMail VM04** | FML-VM04 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 4x vCPU cores |
| **FortiMail VM08** | FML-VM08 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 8x vCPU cores |
| **FortiMail VM16** | FML-VM16 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 16x vCPU cores |
| **FortiMail VM32** | FML-VM32 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 32x vCPU cores |
| **Accessories** | | |
| **Power Supply** | SP-FAD700-PS | AC power supply for FML-400E |
| **Power Supply** | SP-FML900F-PS | AC power supply for FML-400F and FML-900F |
| **Power Supply** | SP-FML2000F-PS | AC power supply for FML-2000F |
| **Power Supply** | SP-FML3000F-PS | AC power supply for FML-3000F and FML-3200F |
| **Hard Drive** | SP-D2TE | 2 TB 3.5" SAS hard drive with tray for FML-2000F, FML-3000F and FML-3200F |
| **Hard Drive** | SP-FAZ1000G-HDD | 4 TB 3.5” SAS SED hard drive with tray for FML-900G |
| **Hard Drive** | SP-FML900F-HDD | 2 TB 3.5" SATA hard drive with tray for FML-900F |
| **Service and Support** | | |
| **Appliances - Hardware plus 24×7 FortiCare and FortiGuard Base Bundle** | | |
| **Appliances - Hardware plus 24×7 FortiCare and FortiGuard Enterprise ATP Bundle** | | |
| **Virtual Machines - 24×7 FortiCare and FortiGuard Base Bundle Contract** | | |
| **Virtual Machines - 24×7 FortiCare and FortiGuard Enterprise ATP Bundle Contract** | | |
| **Microsoft 365 and Google Gsuite Email API Integration Service** | | |
| **Add-on Capabilities** | | |
| **Dynamic Adult Image Analysis Service** | | |
| **Email Continuity** | | |
| **For Service Providers and Enterprises** | | |
| **Advanced Administration License for MSSPs and Enterprises requiring multi-tenancy and additional features** | | |

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

### Fortinet Corporate Social Responsibility Policy

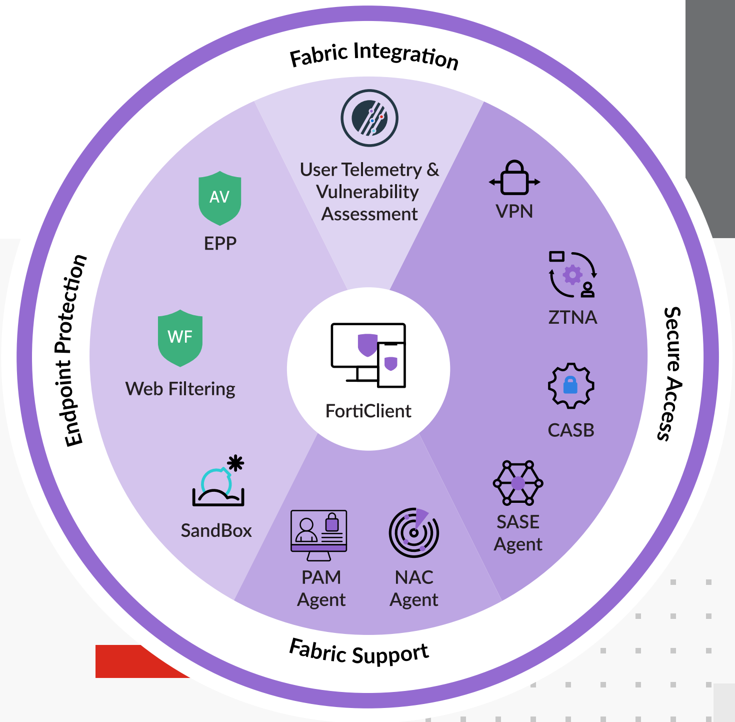
Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

September 3, 2025

# FortiClient

The Fortinet Unified Agent



## Highlights

- ZTNA Agent
- SASE Agent
- Endpoint Protection (EPP)
- Vulnerability Assessment
- Security Fabric Agent
- VPN Agent
- Sandboxing
- CASB (inline and API)
- Centralized Management, Logging, Reporting
- Managed Services available

## Unified Agent for Visibility and Control, Endpoint Protection, and Secure Remote Access using ZTNA Technologies

The FortiClient platform integration provides endpoint visibility, ensuring all Fortinet Security Fabric components have tracking and awareness, compliance enforcement, and reporting.  These integrations reduce the number of agents deployed as FortiClient is the Unified Agent for Fortinet. Secure remote access to applications is delivered via ZTNA, CASB, or traditional virtual private network (VPN) tunnels. NextGen anti-malware and anti-exploit capabilities provide security and protection for endpoints when local or remote.

## Features

**Unified Endpoint** features including compliance, protection, and secure access into a single modular lightweight client. FortiClient is the agent for VPN, ZTNA, and Security Fabric telemetry and is incorporated into FortiSASE, FortiNAC, and FortiPAM.

**Universal ZTNA**, with automatic, encrypted tunnels for controlled validated adaptive per-session access to applications based on device and user identity verification, near real-time continuous endpoint device security posture checks and granular application access policy regardless of location.

**Advanced Threat Protection** against exploits and advanced malware, powered by FortiGuard along with FortiSandbox integration.

**Simplified Management and Policy Enforcement** with FortiClient EMS, FortiClient Cloud, and FortiGate.

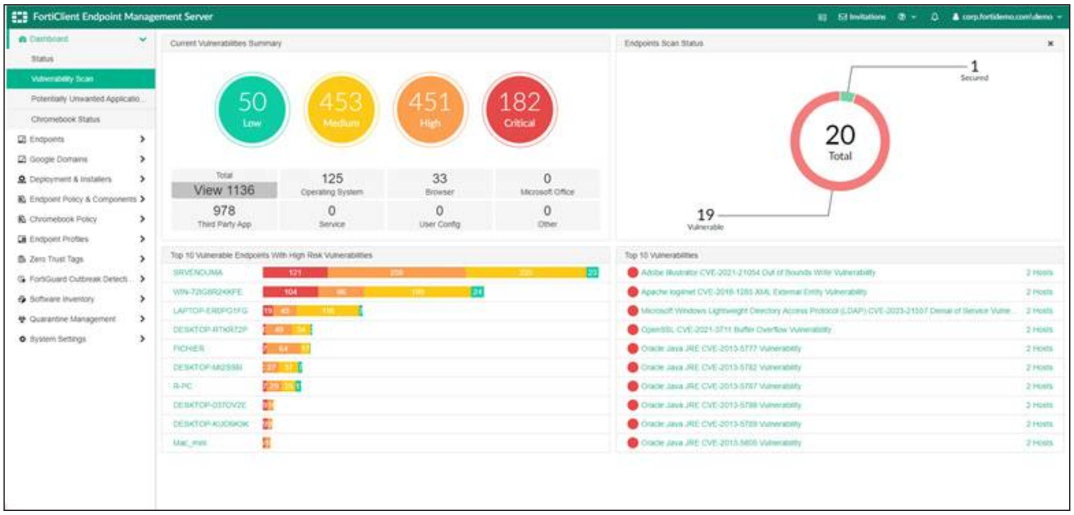
**Available in**

**Virtual**

**Hosted**

## Central Management Tools
## Endpoint Management System (EMS)

- Simple and user-friendly UI
- Remote FortiClient deployment
- ZTNA orchestration
- Real-time dashboard
- Software inventory management
- Active Directory (AD) and Microsoft Entra ID integration
- Central quarantine management
- Automatic group assignment
- Dynamic access control
- Automatic email alerts
- Supports custom groups
- Remote actions
- On-premise and cloud-based options
- Zero trust tagging rules



Current Vulnerabilities Summary

50 Low | 453 Medium | 451 High | 182 Critical

| | | | |
|---|---|---|---|
| Total<br>View 1136 | 125<br>Operating System | 33<br>Browser | 0<br>Microsoft Office |
| 978<br>Third Party App | 0<br>Service | 0<br>User Config | 0<br>Other |

Endpoints Scan Status

Top 10 Vulnerable Endpoints With High Risk Vulnerabilities

Top 10 Vulnerabilities

| | |
|---|---|
| Adobe Illustrator CVE-2021-21054 Out of Bounds Write Vulnerability | 2 Hosts |
| Apache log4net CVE-2018-1285 XML External Entity Vulnerability | 2 Hosts |
| Microsoft Windows Lightweight Directory Access Protocol (LDAP) CVE-2023-21557 Denial of Service Vulne... | 2 Hosts |
| OpenSSL CVE-2021-3711 Buffer Overflow Vulnerability | 2 Hosts |
| Oracle Java JRE CVE-2013-5777 Vulnerability | 2 Hosts |
| Oracle Java JRE CVE-2013-5782 Vulnerability | 2 Hosts |
| Oracle Java JRE CVE-2013-5787 Vulnerability | 2 Hosts |
| Oracle Java JRE CVE-2013-5788 Vulnerability | 2 Hosts |
| Oracle Java JRE CVE-2013-5789 Vulnerability | 2 Hosts |
| Oracle Java JRE CVE-2013-5805 Vulnerability | 2 Hosts |

Vulnerability Dashboard

## Benefits

### Security Fabric Integration

FortiClient integrates endpoints into Fortinet’s Security Fabric for early detection and prevention of advanced threats. This integration delivers native endpoint visibility, compliance control, vulnerability management, and automation. FortiOS and FortiAnalyzer leverage FortiClient endpoint telemetry intelligence to identify indicators of compromise. With the automation capability, administrators can investigate in real time and set policies to automate responses, including quarantining suspicious or compromised endpoints to contain incidents and stem outbreaks. Fortinet’s endpoint compliance and vulnerability management features simplify the enforcement of enterprise security policies preventing endpoints from becoming easy attack targets.

### Universal ZTNA

FortiClient Universal ZTNA works with FortiOS to enable secure granular access to applications no matter if the user is local or remote. Each session is initiated with an automatic, encrypted tunnel from FortiClient to the FortiOS ZTNA Application Gateway for user and device identity verification. In addition, FortiClient performs continuous near real-time endpoint posture checks that enables ZTNA application gateway to provide adaptive real-time access control based on dynamic endpoint posture validation. You can also use multi-factor authentication to provide an additional layer of security. With Universal ZTNA, organizations benefit from not only more secure and better remote access but in addition can offer consistent security and user experience for secure access to applications for on-prem and remote users regardless of endpoint location.

### Unified Agent

FortiClient is the Fortinet Unified Agent platform, acting as that bit of code running on the laptop or mobile device that is needed for many cybersecurity products, thereby reducing ‘agent sprawl’. In addition to the features and benefits of FortiClient itself, the FortiClient Agent can also provide support for FortiSASE, FortiNAC, FortiPAM, and FortiMontior. In the case of FortiSASE, a FortiSASE license includes FortiClient. FortiClient only loads the elements needed, so it remains as lightweight as possible.

### Web Filtering and SaaS Control

FortiClient provides remote web and video filtering, delivering web security and content filtering. This function provides phishing and botnet protection as well as granular application traffic control including web-based applications, YouTube, and software as a service (SaaS).

### Vulnerability Assessment

FortiClient can reduce the attack surface by scanning endpoints for vulnerabilities and sharing that information for appropriate action. Any vulnerabilities can be leveraged by firewall policies, by ZTNA policies, or could result in quarantining of the endpoint.

## Benefits continued

### Patch Policy Enforcement

Keeping endpoints up to date with the latest firmware can be difficult.  FortiClient simplifies this task by managing endpoint patching, even when the endpoints are not on the network.

### Malware and Exploit Prevention

By integrating with FortiClient Cloud Sandbox and leveraging FortiGuard global threat intelligence, FortiClient prevents advanced malware and vulnerabilities from being exploited. FortiClient integrates with FortiClient Cloud Sandbox to analyze all files downloaded to FortiClient endpoints in real time. Millions of FortiClient and FortiSandbox users worldwide share information about known and newly discovered malware with the cloud-based FortiGuard threat intelligence platform that eventually turns into usable threat intelligence.

### Ransomware Protection

FortiClient contains behavior-based ransomware protection, with the ability to roll back changes made by malicious programs, putting the endpoint back to a preinfection state.

### Flexible Licensing

FortiClient is available through either the traditional device-based licensing or user-based FortiTrust licensing. Both options offer the same functionality and allow customers to decide how they want to subscribe to the benefits of FortiClient. FortiFlex for MSSPs is also available for MSSPs to enable them to offer FortiClient to their customers on a subscription model.

### VPN

FortiClient provides flexible options for VPN connectivity. The split tunneling feature enables remote users on VPNs to access the Internet without their traffic having to pass through the corporate VPN headend, as in a typical VPN tunnel. This feature reduces latency, which improves user experience. At the same time, FortiClient includes protections to ensure that Internet-based transactions cannot backflow into the VPN connection and jeopardize the corporate network.

In addition to simple remote connectivity, FortiClient simplifies the remote user experience with features such as autoconnect and always-on VPN, as well as dynamic VPN gate selection. You can also use multifactor authentication to provide an additional layer of security. Having VPN and ZTNA with the same agent simplifies and de-risks the transition to ZTNA.

FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide 24/7 Support
support.fortinet.com

# FortiClient Services

## FortiClient Managed Services

To assist and offload busy IT teams, Fortinet is offering FortiClient Managed services to streamline the configuration, deployment, and monitoring of FortiClient agents. Services included with this offering include the following activities.

FortiClient Managed Services include: cloud provisioning, onboarding, vulnerability monitoring, setup and integration.

### Initial FortiClient Cloud Provisioning

The managed services team works with customers to set up and configure their FortiClient Cloud environment for the following capabilities:

- Endpoint groups setup
- ZTNA
- VPN
- Anti-ransomware and malware protection
- Vulnerability management
- Security profiles and policies configuration
- Endpoint posture check rules
- Custom FortiClient installer creation and ongoing installer updates

### Endpoint Onboarding

The managed services team creates custom FortiClient installers for customer-specific use cases, sends invitation emails to users, and onboards them for FortiClient Cloud management and provisioning.

### Security Fabric Setup and Integration

The managed services team integrates FortiClient Cloud with the Fortinet Security Fabric to support uses cases such as ZTNA, incident response, and automation.

### Endpoint Vulnerability Monitoring

The managed services team monitors customer endpoints to identify high-risk endpoints and alert them of endpoints with critical and high vulnerabilities that would be easy targets for cyber attacks. The managed services team detects, reports, and guides customers to remediate those vulnerable endpoints.

## Additional Services

### Best Practice Service (BPS)

Access global knowledge of Fortinet customer best practices.

FortiClient Best Practices Service is an account-based annual subscription providing access to a specialized team that delivers remote guidance on deployment, upgrades, and operations. The service allows customers to share information about their deployment, user requirements, resources, and other related items. Based on the information provided, the BPS experts can provide recommended best practices, sample code, links to tools, and other materials or assistance to speed adoption and guide the customer towards best practice deployments. The team does not log into customer devices to make changes for them. This approach is a consulting and guidance service which may include sample configurations or playbooks. This approach is not an on-site professional services offer.

### FortiClient Forensics Analysis Service

Extend your IT team with skilled FortiClient specialists.

FortiClient Forensic Service provides analysis from remote FortiGuard Labs experts to help endpoint customers respond to and recover from cyber incidents. For each engagement, forensic analysts from Fortinet's FortiGuard Labs will assist in the collection, examination, and presentation of digital evidence, including a final, detailed report. FortiClient subscriptions that include Forensic Services entitle the customer to call on these endpoint forensic experts whenever an event happens, offloading internal teams and accelerating investigations by analysts deeply familiar with the tools of endpoint security. Forensics Analysis Service is an annual subscription, not a per-incident license.

### Fortinet CASB Service

Provide visibility, compliance, data security and threat protection.

To safely embrace the cloud, a Cloud Access Security Broker (CASB) can act as a gatekeeper by providing visibility, control, and protection to allow organizations to extend their security policies beyond their own infrastructure. CASB sits between cloud service users and secures SaaS cloud applications, monitors all activity, and enforces security policies. Fortinet's dual mode solution provides security, scalability, and performance using both inline and API-based CASB protections to address all cloud security needs. A FortiClient license enables inline CASB services on a FortiGate and provides a license for FortiCASB, Fortinet's API-based CASB service.

# Feature Highlights

Central management tools provide the ability to centrally manage Windows, macOS, Linux, Chrome, iOS, and Android endpoints. FortiClient EMS provides on-premise management and FortiClient Cloud provides cloud-based management.

## Central Management Tools

**Software Inventory Management** provides visibility into installed software applications and license management to improve security hygiene. You can use inventory information to detect and remove unnecessary or outdated applications that might have vulnerabilities to reduce your attack surface.

**Windows AD Integration** helps sync organizations' AD structure into the central management tools so that you use the same organizational units from your AD server for simplified endpoint management.

**Real-time Endpoint Status** always provides current information on endpoint activity and security events.

**Vulnerability Dashboard** helps manage organizations attack surface. All vulnerable endpoints are easily identified for administrative action.

**Centralized FortiClient Deployment and Provisioning** that allows administrators to remotely deploy endpoint software and perform controlled upgrades. Makes deploying FortiClient configuration to thousands of clients an effortless task with a click of a button.

**FortiSandbox integrations** assist with configuration and suspicious file analysis. Sandbox settings are synchronized across managed endpoints, simplifying setup. A detailed analysis of FortiClient submitted files is available in the central management tools. Administrators can see all the behavior activity of a file, including graphic visualization of the full process tree.

FortiGate provides awareness and control over all your endpoints.

## FortiGate Integrations

**Telemetry** provides real-time endpoint visibility (including user avatar) on FortiGate console so administrators can get a comprehensive view of the whole network. Telemetry also ensures that all fabric components have a unified view of the endpoints.

**Dynamic Access Control for Compliance Enforcement** requires EMS to create virtual groups based on endpoint security posture. These virtual groups are then retrieved by FortiGate and used in firewall policy for dynamic access control. Dynamic groups help automate and simplify compliance to security policies.

**Endpoint Quarantine** helps to quickly disconnect a compromised endpoint from the network and stop it from infecting other assets.

**Automated Response** helps detect and isolate suspicious or compromised endpoints without manual intervention.

**Application-Based Split Tunnel** supports source application-based split tunnel, where you can specify application traffic to exclude from the VPN tunnel, such as high bandwidth apps.

**Web Filtering with Keyword Search / YouTube Filters** blocks web pages containing words or patterns that you specify as well as limit users' access by blocking or only allowing specified YouTube channels.

## Feature Highlights continued

### FortiSASE Integrations

**The FortiSASE license** includes a license for FortiClient, which is the endpoint agent for the FortiSASE solution.

**Endpoint management** is handled by an EMS instance within FortiSASE so that all the FortiClients associated with FortiSASE are properly registered and managed.

**Automatic encrypted tunnels** are created between FortiClient and the FortiSASE Points of Presence (PoPs).

**Vulnerability assessments** conducted by FortiClient are passed to FortiSASE for evaluation as part of ZTNA application access controls.

**Endpoint Protection (EPP)** is included with the FortiClient license, providing more protection for laptops and mobile phones.

# Bundles

| FORTICLIENT EDITION | VPN / ZTNA | EPP / ATP | Managed Services | Chromebook |
|---|---|---|---|---|
| Zero Trust Security | Windows, macOS, Linux | Windows, macOS, Linux | Windows, macOS, Linux | Chromebook |
| Zero Trust Agent with MFA | ✓ | ✓ | ✓ | |
| Security Posture Tagging Rules | ✓ | ✓ | ✓ | |
| Central Management via EMS or FortiClient Cloud | ✓ | ✓ | ✓ | ✓ |
| Dynamic Security Fabric Connector | ✓ | ✓ | ✓ | |
| Vulnerability Agent and Remediation | ✓ | ✓ | ✓ | |
| SSL VPN with MFA | ✓ | ✓ | ✓ | |
| IPSEC VPN with MFA | ✓ | ✓ | ✓ | |
| FortiGuard Web and Video Filtering | ✓ | ✓ | ✓ | ✓ |
| Cloud Access Security Broker (CASB)[1] | ✓ | ✓ | ✓ | |
| FortiPAM Support | ✓ | ✓ | ✓ | |
| Central Logging and Reporting[2] | ✓ | ✓ | ✓ | ✓ |
| Next Generation Endpoint Security | | | | |
| Potentially Unwanted Applications | | ✓ | ✓ | |
| AI powered NGAV | | ✓ | ✓ | |
| Removable Media Control | | ✓ | ✓ | |
| Automated Endpoint Quarantine | | ✓ | ✓ | |
| Application Firewall[3] | | ✓ | ✓ | |
| Software Inventory | | ✓ | ✓ | |
| Ransomware Protection[4] | | ✓ | ✓ | |
| FortiClient Cloud Sandbox (SaaS)[3] | | ✓ | ✓ | |
| FortiSandbox Integration (PaaS/Public Cloud/On-premises)[3] | ✓ | ✓ | ✓ | |
| Managed FortiClient Service | | | | |
| Endpoint Onboarding | | | ✓ | |
| Initial Provisioning | | | ✓ | |
| Security Fabric Setup/Integration | | | ✓ | |
| Vulnerability Monitoring | | | ✓ | |
| Endpoint Security Monitoring | | | ✓ | |
| Additional Services | | | | |
| Best Practice Service (BPS) Consultation | Account add-on | Account add-on | N/A | Account add-on |
| 24×7 Support | ✓ | ✓ | ✓ | ✓ |
| On-Premise/Air Gap Option | ✓ | ✓ | | ✓ |
| FortiGuard Forensics Analysis Service Option | Account add-on | Account add-on | Account add-on | Account add-on |

[1] A license for Inline CASB and FortiCASB (API based) is included.

[2] Requires FortiAnalyzer.

[3] FortiClient (Linux) does not support Sandbox integration.

[4] Only FortiClient (Windows) supports this feature.

# Features Per Platform and Requirements

| | WINDOWS | MACOS | ANDROID | IOS | CHROMEBOOK | LINUX |
|---|---|---|---|---|---|---|
| **Zero Trust Security** | | | | | | |
| **ZTNA Remote Access** | ✓ | ✓ | ✓ | ✓ | | ✓ |
| **Endpoint Telemetry**[1] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Web Filter**[2] | ✓ | ✓ | ✓ | ✓ | ✓ | |
| **Security Posture Tags for Compliance**[1] | ✓ | ✓ | ✓ | ✓ | | ✓ |
| **Endpoint Audit and Remediation with Vulnerability Scanning** | ✓ | ✓ | | | | ✓ |
| **IPSec VPN** | ✓ | ✓ | | ✓ | | ✓ |
| **SSL VPN**[4] | ✓ | ✓ | ✓ | ✓ | ✓[5] | ✓ |
| **Security Posture Tag Check before VPN** | ✓ | ✓ | | | | ✓ |
| **Windows AD SSO Agent** | ✓ | ✓ | | | | |
| **FortiPAM Agent** | ✓ | | | | | |
| **Remote Logging and Reporting**[3] | ✓ | ✓ | | ✓ | ✓ | ✓ |
| **Endpoint Security** | | | | | | |
| **Antivirus** | ✓ | ✓ | | | | ✓ |
| **Cloud-based Threat Detection** | ✓ | ✓ | | | | |
| **Sandbox integration (on-premise)** | ✓ | ✓ | | | | |
| **Sandbox integration (Saas/Paas)** | ✓ | ✓ | | | | |
| **Automated Endpoint Quarantine** | ✓ | ✓ | | | | |
| **AntiExploit** | ✓ | | | | | |
| **Application Firewall** | ✓ | ✓ | | | | |
| **Potentially Unwanted Applications** | ✓ | ✓ | | | | |
| **FortiClient Forensic Analysis** | ✓ | ✓ | | | | ✓ |
| **Removable Media Control** | ✓ | ✓ | | | | ✓ |

1. Requires EMS or FortiClient Cloud to centrally manage FortiClient.

2. Also compatible with Chrome OS.

3. Requires FortiAnalyzer.

4. Also compatible with Windows mobile.

5. Free Android SSL VPN Client available in Google Play Store.

The above list is based on the latest OS for each platform.

| FORTICLIENT |
|---|
| **Supported Operating Systems** |
| Microsoft Windows 10 (32-bit and 64-bit) ARM* |
| Microsoft Windows 11 (64-bit) |
| Microsoft Windows Server 2019 or later |
| macOS 10.15 or later |
| iOS 9.0 or later |
| Android 5.0 or later |
| Linux Ubuntu 22.04 and later, Red Hat 9 and later, CentOS 9.0 and later with KDE or GNOME |
| All Chromebook versions |
| **Authentication Options** |
| RADIUS, LDAP, local database, xAuth, TACACS+, digital certificate (X509 format), FortiToken |
| **Connection Options** |
| Autoconnect VPN before Windows logon |
| IKE mode configuration for FortiClient IPsec VPN tunnel |

* ARM-based processor support is in beta. As such, for ARM-based processors, FortiClient (Windows) supports a limited feature set as follows:

Fortinet Security Fabric agent (connection to EMS and Telemetry)

Remote Access (VPN)

Web Filter

Vulnerability Scan

| FORTICLIENT EMS |
|---|
| **Supported Operating Systems** |
| Windows Server 2022 or later OR Ubuntu 22.04 LTS Server or Ubuntu 24.04 LTS |
| **Endpoint Requirement** |
| FortiClient 7.2 or later, FortiClient for Windows and macOS X, 7.0 for iOS and Android |
| **System Requirements** |
| 2.0 GHz 64-bit processor, six virtual CPUs |
| 12 GB RAM |
| 80 GB free hard disk |
| Gigabit (10/100/1000baseT) Ethernet adapter |

# Order Information

You can order FortiClient based on the number of devices. The following table reflects the latest FortiClient device-based license packs.

| EDITION | VPN/ZTNA | VPN/ ZTNA + EPP/ ATP | MANAGED | CHROMEBOOK |
|---|---|---|---|---|
| SaaS (Cloud Hosted EMS) | | | | |
| 25-pack | FC1-10-EMS05-428-01-DD | FC1-10-EMS05-429-01-DD | FC1-10-EMS05-485-01-DD | FC1-10-EMS05-403-01-DD |
| 500-pack | FC2-10-EMS05-428-01-DD | FC2-10-EMS05-429-01-DD | FC2-10-EMS05-485-01-DD | FC2-10-EMS05-403-01-DD |
| 2000-pack | FC3-10-EMS05-428-01-DD | FC3-10-EMS05-429-01-DD | FC3-10-EMS05-485-01-DD | FC3-10-EMS05-403-01-DD |
| 10 000 pack | FC4-10-EMS05-428-01-DD | FC4-10-EMS05-429-01-DD | FC4-10-EMS05-485-01-DD | FC4-10-EMS05-403-01-DD |
| On Premise | | | | |
| 25-pack | FC1-10-EMS04-428-01-DD | FC1-10-EMS04-429-01-DD | | FC1-10-EMS04-403-01-DD |
| 500-pack | FC2-10-EMS04-428-01-DD | FC2-10-EMS04-429-01-DD | | FC2-10-EMS04-403-01-DD |
| 2000-pack | FC3-10-EMS04-428-01-DD | FC3-10-EMS04-429-01-DD | | FC3-10-EMS04-403-01-DD |
| 10 000 pack | FC4-10-EMS04-428-01-DD | FC4-10-EMS04-429-01-DD | | FC4-10-EMS04-403-01-DD |
| FortiCare Best Practices Consultation Service | | | | |
| 25-999 endpoints | FC1-10-FCBPS-310-02-DD | | | |
| 1000-9999 endpoints | FC2-10-FCBPS-310-02-DD | | | |
| 10 000+ endpoints | FC5-10-FCBPS-310-02-DD | | | |
| Training Services | | | | |
| Classroom - virtual ILT | FT-FCT | | | |
| Lab access - standard NSE training lab environment | FT-FCT-LAB | | | |
| NSE5 exam voucher | NSE-EX-SPL5 | | | |

You can order FortiClient based on the number of users. The following table reflects the latest FortiTrust user-based license ranges.

| FORTITRUST USER-BASED LICENSE RANGES* | | | | |
|---|---|---|---|---|
| SOLUTION | SKU LICENSE | VPN/ ZTNA | VPN/ ZTNA + EPP/ ATP | MANAGED VPN/ ZTNA + EPP/ ATP |
| Cloud-hosted EMS | 50-499 users | FC2-10-EMS05-509-02-DD | FC2-10-EMS05-546-02-DD | FC2-10-EMS05-556-02-DD |
| | 500-1999 users | FC3-10-EMS05-509-02-DD | FC3-10-EMS05-546-02-DD | FC3-10-EMS05-556-02-DD |
| | 2000-9999 users | FC4-10-EMS05-509-02-DD | FC4-10-EMS05-546-02-DD | FC4-10-EMS05-556-02-DD |
| | 10 000+ users | FC5-10-EMS05-509-02-DD | FC5-10-EMS05-546-02-DD | FC5-10-EMS05-556-02-DD |

* A user-based license allows a single user to install and use FortiClient on up to three devices.

The following table reflects the latest licenses for the Forensic Analysis Service.

| FORENSIC ANALYSIS SERVICE | | | | |
|---|---|---|---|---|
| SOLUTION | SKU LICENSE | VPN/ ZTNA | VPN/ ZTNA + EPP/ ATP | MANAGED VPN/ ZTNA + EPP/ ATP |
| Device-based Licenses | 25-pack | FC1-10-EMS05-537-01-DD | FC1-10-EMS05-538-01-DD | FC1-10-EMS05-539-01-DD |
| | 500-pack | FC2-10-EMS05-537-01-DD | FC2-10-EMS05-538-01-DD | FC2-10-EMS05-539-01-DD |
| | 2000-pack | FC3-10-EMS05-537-01-DD | FC3-10-EMS05-538-01-DD | FC3-10-EMS05-539-01-DD |
| | 10 000-pack | FC4-10-EMS05-537-01-DD | FC4-10-EMS05-538-01-DD | FC4-10-EMS05-539-01-DD |
| FortiTrust<br>(User-based Licenses) | 100-499 users | FC2-10-EMS05-557-02-DD | FC2-10-EMS05-558-02-DD | FC2-10-EMS05-559-02-DD |
| | 500-1999 users | FC3-10-EMS05-557-02-DD | FC3-10-EMS05-558-02-DD | FC3-10-EMS05-559-02-DD |
| | 2000-9999 users | FC4-10-EMS05-557-02-DD | FC4-10-EMS05-558-02-DD | FC4-10-EMS05-559-02-DD |
| | 10 000+ users | FC5-10-EMS05-557-02-DD | FC5-10-EMS05-558-02-DD | FC5-10-EMS05-559-02-DD |

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

FORTINET

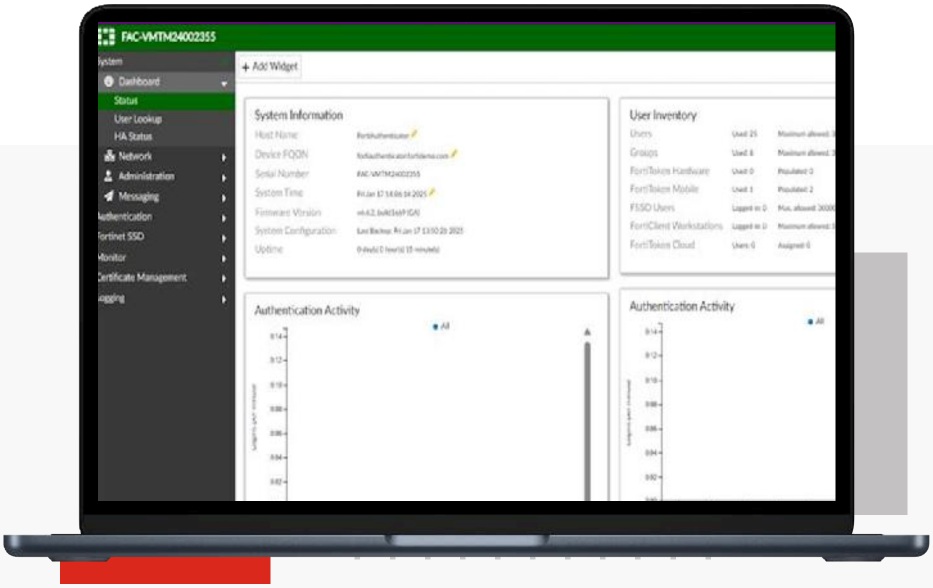
www.fortinet.com

August 25, 2025

Data Sheet

# FortiAuthenticator™

## Identity and Access Management



System Information

| | |
|---|---|
| Host Name | fortiauthenticator |
| Device FQDN | [illegible] |
| Serial Number | FAC-VMTM24002355 |
| System Time | Fri Jan 17 14:06:14 2025 |
| Firmware Version | [illegible] |
| System Configuration | Last Backup: Fri Jan 17 13:50:20 2025 |
| Uptime | 0 day(s) 0 hour(s) 15 minute(s) |

User Inventory

| | | |
|---|---|---|
| Users | Used: 25 | Maximum allowed: [illegible] |
| Groups | Used: 8 | Maximum allowed: [illegible] |
| FortiToken Hardware | Used: 0 | Populated: 0 |
| FortiToken Mobile | Used: 1 | Populated: 2 |
| FSSO Users | Logged in: 0 | Max. allowed: [illegible] |
| FortiClient Workstations | Logged in: 0 | Maximum allowed: [illegible] |
| FortiToken Cloud | Users: 0 | Assigned: 0 |

### Highlights

- Centralized user authentication and authorization
- Multi-factor authentication (MFA)
- Single Sign-On (SSO)
- FIDO passwordless registration and authentication
- Certificate management
- RADIUS, TACACS+, LDAP, SAML IdP and SP support
- Fortinet Single Sign-On (FSSO)
- Trusted Endpoint SSO

## Centralized Identity and Access Management Solution

Network and Internet access is key for almost every role within the enterprise; however, this requirement must be balanced with the risk that it brings. The key objective of every enterprise is to provide secure but controlled network access enabling the right person the right access at the right time, without compromising on security.

FortiAuthenticator is a scalable Identity and Access Management (IAM) solution that enhances security and simplifies authentication for enterprises. Available as a physical or virtual appliance for private and public cloud deployments, it provides robust services such as RADIUSTACACS+ service, Multi-Factor Authentication (MFA), Passwordless Authentication, Adaptive Authentication (AA), Single Sign-On (SSO), Identity Provider (IdP), and IdP Proxy, System for Cross Identity Management (SCIM), Fortinet Single Sign-On (FSSO), and Certificate Authority.

FortiAuthenticator integrates seamlessly with remote on-prem and cloud directories, applications, and Fortinet's Security Fabric. This entegration ensures secure and streamlined access to business resources and internal and external SaaS applications (e.g., Microsoft 365). Supporting legacy and modern authentication protocols, including FIDO passkeys, FortiAuthenticator employs context-aware, adaptive authentication to grant, challenge, or deny access based on login criteria. Acting as a gatekeeper, it identifies users, queries third-party access permissions, and communicates identity-based policies to FortiGate devices, securing enterprise networks with precision and ease.

Available in:

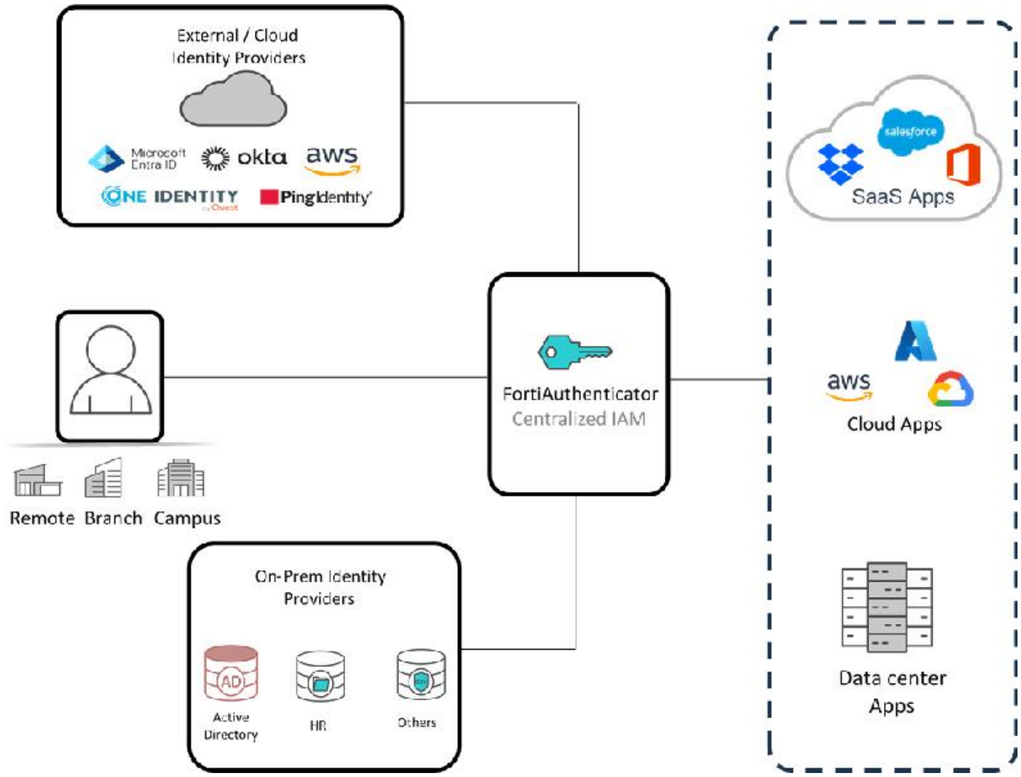
Appliance

Virtual Machine

Hosted

Cloud

## Solution Deployment



## Features

### Centralized Authentication

FortiAuthenticator streamlines and secures user authentication by acting as a standalone IdP or integrating with both on-premises and cloud identity providers, offering seamless access to systems and applications for users, regardless of location. It supports a wide range of multi-factor authentication (MFA) methods, including FortiToken, SMS and email OTP, and FIDO2 for passwordless authentication, delivering a consistent, secure, and unified authentication experience. By centralizing authentication, FortiAuthenticator enhances security across the organization, improves operational efficiency, and reduces the complexity associated with managing multiple disparate authentication systems.

FortiAuthenticator integrates seamlessly with multiple Fortinet products and services, providing identity management and strong authentication across Fortinet's Security Fabric. Additionally, it functions as a fully standalone authentication solution for third-party environments, supporting RADIUS and LDAP authentication and SAML and OAuth/OIDC SSO. This flexibility allows organizations to implement FortiAuthenticator in both Fortinet-centric and heterogeneous IT infrastructures with ease.

### Strong User Identity with Multi-Factor Authentication (MFA)

FortiAuthenticator enhances user security by enforcing robust multi-factor authentication (MFA) to secure access to critical resources. It supports a diverse range of MFA methods, including FortiToken Mobile and hardware tokens, SMS and email OTP, client certificate-based authentication, and FIDO2 for passwordless authentication, ensuring flexible and secure user verification across all scenarios.

By combining user identity information with authentication data from FortiToken or FIDO2 services, FortiAuthenticator ensures only authorized individuals gain access, reducing the risk of unauthorized access and data breaches. This added layer of security also helps organizations comply with government and business privacy regulations.

With the industry's widest range of MFA options, FortiAuthenticator accommodates diverse user needs, offering time-based physical tokens, mobile apps (iOS, Android, Windows), and modern passwordless methods like FIDO2. Its capabilities extend to controlling access for FortiGate management, SSL/IPsec VPNs, wireless captive portals, third-party RADIUS-compliant networking equipment, and SAML service providers.

FortiAuthenticator also features a REST API for adding MFA to custom web-based applications, enabling seamless integration into existing workflows. To simplify local user management, it includes self-registration and password recovery capabilities, ensuring a streamlined and user-friendly experience.

# Features

### Certificate Management

FortiAuthenticator serves as a robust Certificate Authority (CA), enabling administrators to create, import, and manage X.509 certificates, including server certificates for HTTPS and SSH, and client certificates for HTTPS, SSL, and IPsec VPNs. It supports the full certificate lifecycle, including generation, signing, and revocation, and offers streamlined management of Certificate Revocation Lists (CRLs).

To ensure secure and automated certificate operations, FortiAuthenticator supports SCEP and CMP protocols, simplifying certificate deployment and renewal processes. It integrates seamlessly with remote LDAP servers, verifying identities using trusted CA certificates, and supports EAP authentication by validating client certificates against authorized CA certificates and user records.

In environments with site-to-site VPNs, where pre-shared keys can pose a security risk, FortiAuthenticator enhances security by enabling certificate-based VPNs. Its integration with FortiManager automates bulk certificate deployment and simplifies certificate management, removing the complexity traditionally associated with these solutions. Certificates are securely delivered via the SCEP protocol, making it easier to implement and manage certificate-secured VPNs within FortiGate environments.

For client-based VPNs, FortiAuthenticator supports the FortiToken 300 USB Certificate Store, a secure, PIN-protected hardware solution that enhances client VPN security. This USB-based certificate store is fully compatible with FortiClient, ensuring an additional layer of protection for client VPN connections.

### Adaptive Authentication

FortiAuthenticator provides advanced adaptive authentication capabilities by analyzing contextual factors during login, such as user location, device type, time of day, behavior patterns, and IP address. Based on this context and predefined policies, it dynamically adjusts authentication requirements, such as enforcing MFA, bypassing MFA, or blocking access entirely. This approach ensures secure, context-aware access control, allowing organizations to apply stricter security measures or deny access based on risk. These adaptive features enable organizations to strengthen security while maintaining a seamless user experience.

### Protocol Support for Flexible Integration

FortiAuthenticator is designed for interoperability, supporting a wide range of protocols including RADIUS, SAML, OIDC, LDAP, and TACACS+. This extensive protocol compatibility ensures seamless integration with diverse systems, allowing organizations to leverage existing infrastructure while enhancing security and scalability.

# Features

### 802.1X Authentication

FortiAuthenticator supports 802.1X authentication, a foundational protocol for enterprise network access control. Acting as a RADIUS server, it provides authentication, authorization, and accounting (AAA) services for devices connecting to wired, wireless, or VPN networks. By validating user credentials, device certificates, or both, FortiAuthenticator ensures that only authorized users and devices gain access, effectively preventing unauthorized network access.

FortiAuthenticator integrates seamlessly with existing identity stores such as Active Directory, LDAP, and PKI systems, and supports advanced protocols like EAP-TLS for certificate-based authentication. These capabilities enable enterprises to enforce Zero Trust principles, ensure compliance with security policies, and safeguard sensitive resources against unauthorized access.

With FortiAuthenticator, organizations can achieve secure port-level access control for LAN and WLAN environments, offering robust protection for enterprise networks while supporting scalable and flexible deployment options.

### TACACS+ and RADIUS Authentication

Serving as a centralized Authentication, Authorization, and Accounting (AAA) server, FortiAuthenticator supports both TACACS+ and RADIUS protocols. This approach enables secure network access control by authenticating users and devices, enforcing access policies, and providing granular control over network commands and configurations.

### Single Sign-On (SSO)

FortiAuthenticator can function as a SAML Identity Provider (IdP) or as an IdP proxy, allowing it to federate user and group information from remote IdPs to service providers (SPs) (including FortiGate). It supports both SP-initiated and IdP-initiated login flows, ensuring compatibility with a wide range of systems. Additionally, FortiAuthenticator can serve as an OIDC Provider, making it ideal for scenarios involving mobile and native applications.

### Trusted Endpoint SSO

FortiAuthenticator’s Trusted Endpoint SSO feature enhances seamless and secure user authentication by leveraging FortiClient EMS and ZTNA. Once users log in to their endpoint devices, their credentials are securely cached by FortiAuthenticator, allowing for transparent authentication to service providers without requiring repeated logins.

This feature integrates device security posture checks from FortiClient EMS, ensuring only trusted and compliant endpoints are granted access. It enhances user experience, reduces friction during authentication, and enforces Zero Trust principles by validating both user identity and device trustworthiness. This feature makes Trusted Endpoint SSO a valuable differentiator for organizations prioritizing secure, user-friendly access.

# Features

### Fortinet Single Sign-On (FSSO)

Fortinet Single Sign-On (FSSO) is a proprietary feature that enables seamless and transparent user authentication for FortiGate firewalls. By collecting user, IP, and group information from external identity sources such as Active Directory or LDAP, FSSO allows FortiGate devices to enforce identity-based policies for network access control. FortiAuthenticator serves as a central collector for user authentication events, channeling login and logout status from various sources and ensuring accurate identity tracking across Fortinet deployments.

FortiAuthenticator’s FSSO capability ensures consistent and centralized user identity management for FortiGate deployments. By supporting multiple authentication methods and integrating with diverse directory systems, it provides flexibility for complex network environments. This approach not only enhances security by enabling identity-based policies but also improves the user experience with transparent authentication processes.

### Key Features of FortiAuthenticator FSSO Integration:

1. **Active Directory Polling:** FortiAuthenticator detects user logins by regularly polling Active Directory domain controllers. Once a login is identified, it collects the username, IP address, and group details, storing them in the FortiAuthenticator User Identity Management Database. These details can then be shared with multiple FortiGate devices to enforce identity-based policies.
2. **FortiAuthenticator SSO Mobility Agent**: For distributed or complex domain environments where polling domain controllers is impractical, the FortiAuthenticator SSO Mobility Agent provides an alternative. Distributed via FortiClient or as a standalone application, it communicates login events, IP changes (e.g., between wired and wireless networks), and logout events to FortiAuthenticator, ensuring real-time user tracking without relying on polling.
3. **Explicit Authentication Portal and Widgets**: For systems that do not support AD polling or where an SSO client is not feasible, FortiAuthenticator offers a user authentication portal. Users can manually log in to gain network access, and to streamline repeated logins, organizations can deploy widgets on their intranet. These widgets leverage browser cookies to automatically log in users when they access the intranet homepage.
4. **RADIUS Accounting Integration**: In networks utilizing RADIUS authentication (e.g., for wireless or VPN access), RADIUS Accounting can serve as a user identification method. FortiAuthenticator uses this information to detect logins, associate IP and group details with users, and eliminate the need for redundant authentication tiers.

## Features

### System for Cross-domain Identity Management (SCIM)

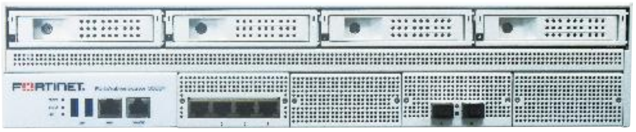
FortiAuthenticator supports SCIM, an open standard for automating the exchange of user identity information between identity providers and service providers. This method facilitates seamless synchronization of user data, streamlining provisioning and deprovisioning processes, and reducing administrative overhead.

### Offline Token Provisioning for Air-Gapped Environments

FortiAuthenticator ensures secure authentication even in air-gapped environments by supporting offline token provisioning. Administrators can activate FortiToken Mobile tokens without internet connectivity through QR codes or manual activation codes. This feature is particularly valuable for operational technology (OT) networks and other isolated environments where internet access is restricted, providing robust authentication while maintaining strict network isolation and security.

FortiAuthenticator 300F

FortiAuthenticator 800F



FortiAuthenticator 3000F

# Specifications

| FORTIAUTHENTICATOR MODEL NO. | FAC-300F | FAC-800F | FAC-3000F |
|---|---|---|---|
| **Hardware** | | | |
| **10/100/1000 Interfaces (Copper, RJ-45)** | 4 | 4 | 4 |
| **SFP Interfaces** | 0 | 2 | 2 |
| **Local Storage** | 2× 1TB Hard Disk Drive - RAID 1 | 2× 2 TB Hard Disk Drive - RAID 1 | 2× 2 TB SAS Drive - RAID 1 |
| **Trusted Platform Module (TPM)** | Yes | Yes | Yes |
| **Power Supply** | 300W Redundant Auto Ranging (100V-240V), Optional Dual (1+1) | Dual (1+1) 300W Redundant Auto Ranging (100V–240V) | Dual (1+1) 1000W Auto Ranging (100V–240V) |
| **System Capacity** | | | |
| **Local + Remote Users (Base / Upper Limit)** | 1500 / 3500 | 8000 / 18 000 | 40 000 / 240 000 |
| **FortiTokens** | 3000 | 16 000 | 480 000 |
| **RADIUS Clients (NAS Devices) (Base / Upper Limit)** | 500 / 1166 | 2666 / 6000 | 13 333 / 80 000 |
| **User Groups** | 150 | 800 | 24 000 |
| **CA Certificates** | 10 | 50 | 300 |
| **User Certificates** | 7500 | 40 000 | 1 200 000 |
| **Dimensions** | | | |
| **Height x Width x Length (inches)** | 1.75 × 17.0 × 15.04 | 1.75 × 17.0 × 27.61 | 3.46 × 17.24 × 23.66 |
| **Height x Width x Length (mm)** | 44 × 438 × 422 | 44 × 438 × 701.2 | 88 × 438 × 601 |
| **Weight** | 18.0 lbs (8.2 kg) | 33.0 lbs (15.0 kg) | 44 lbs (20 kg) |
| **Environment** | | | |
| **Form Factor** | Rack Mountable (1RU) | Rack Mountable (1RU) | Rack Mountable (2 RU) |
| **Power Source** | 100-240 VAC, 50/60 Hz 300W Redundant (1+0) | 100–240V AC, 50/60 Hz | 100–240V AC, 50–60 Hz |
| **Maximum Current** | 5A /100V, 2.5A /240V | 5A /100V, 2.5A /240V | 100-127/200-240VAC, 50/60Hz, 10/5A |
| **Power Consumption (Average / Maximum)** | 82.35 W / 131.23 W | 154 W / 196.04 W | 193.30 W / 236.28 W |
| **Heat Dissipation** | 482 BTU/h | 703 BTU/h | 1325 BTU/h |
| **Forced Airflow** | Front to back | Front to back | Front to back |
| **Noise Level** | | | 49.8 db |
| **Operating Temperature** | 32°–104°F (0°–40°C) | 32°–104°F (0°–40°C) | 32°–104°F (0°–40°C) |
| **Storage Temperature** | -4°–158°F (-20°–70°C) | -4°–158°F (-20°–70°C) | -40°–158°F (-40°–70°C) |
| **Humidity** | 5%–90% non-condensing | 5%–95% non-condensing | 5%–90% non-condensing |
| **System** | | | |
| **Standards Supported** | 10/100/1000 Base-TX (GE), IP, Telnet, HTTP 1.0/1.1, SSL, RS232, NTP Client (RFC1305), RADIUS (RFC2865), LDAP (RFC4510), x.509 (RFC5280), Certificate Revocation (RFC3280), PKCS#12 Certificate Import, PKCS#10 CSR Import (RFC2986), Online Certificate Status Protocol (RFC 2560), EAP-TLS (RFC2716), Simple Certificate Enrollment Protocol (SCEP), oAuth, OIDC, and SAML2.0 | | |
| **Management** | CLI, Direct Console DB9 CLI, HTTPS | | |
| **High Availability** | Active-Passive HA and Config Sync HA | | |
| **Compliance** | | | |
| **Safety** | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST | FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST |

# Specifications

| VIRTUAL APPLIANCES | FAC-VM BASE | FAC-VM-100-UG | FAC-VM-1000-UG | FAC-VM-10000-UG |
|---|---|---|---|---|
| **Capacity** | | | | |
| **Users (Local and Remote)** | 100 | +100 | +1000 | +10 000 |
| **FortiTokens** | 200 | +200 | +2000 | +20 000 |
| **NAS Devices** | 33 | +33 | +333 | +3333 |
| **User Groups** | 10 | +10 | +100 | +1000 |
| **CA Certificates** | 5 | +5 | +50 | +500 |
| **User Certificates** | 500 | +500 | +5000 | +50 000 |
| **Virtual Machine** | | | | |
| **Hypervisors Supported** | VMware ESXi/ ESX 6/ 7/ 8, Microsoft Hyper-V Server 2010, 2012 R2, 2016, and 2019, KVM, Xen, Microsoft Azure, AWS, Nutanix AHV (Acropolis Hypervisor), Oracle OCI, Alibaba Cloud | | | |
| **Maximum Virtual CPUs Supported** | 64 | | | |
| **Virtual NICs Required (Minimum / Maximum)** | 1 / 4 | | | |
| **Virtual Machine Storage (Minimum / Maximum)** | 60 GB / 16 TB | | | |
| **Virtual Machine Memory Required (Minimum / Maximum)** | 2 GB / 1 TB | | | |
| **High Availability Support** | Active-Passive HA and Config Sync HA | | | |

## Order Information

| Product | SKU | Description |
|---|---|---|
| **FortiAuthenticator 300F** | FAC-300F | 4x GE RJ45 ports, 2× 1 TB HDD. Base License supports up to 1500 users. Expand user support to 3500 users by using FortiAuthenticator Hardware Upgrade License. |
| **FortiAuthenticator 800F** | FAC-800F | 4x GE RJ45 ports, 2x GE SFP, 2× 2 TB HDD. Base License supports up to 8000 users. Expand user support to 18 000 users by using FortiAuthenticator Hardware Upgrade License. |
| **FortiAuthenticator 3000F** | FAC-3000F | 4x GE RJ45 ports, 2× 10GE SPF, 2× 2TB SAS Drive. Base License supports up to 40 000 users. Expand user support to 240 000 users by using FortiAuthenticator Hardware Upgrade License |
| **FortiAuthenticator-VM License** | FAC-VM-Base | VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License. |
| | FAC-VM-100-UG | FortiAuthenticator-VM 100 user license upgrade. |
| | FAC-VM-1000-UG | FortiAuthenticator-VM 1000 user license upgrade. |
| | FAC-VM-10000-UG | FortiAuthenticator-VM 10 000 user license upgrade. |
| | FC1-10-0ACVM-248-02-12 | 1 Year 24×7 FortiCare Contract (1–500 users). |
| | FC2-10-0ACVM-248-02-12 | 1 Year 24×7 FortiCare Contract (1–1100 users). |
| | FC3-10-0ACVM-248-02-12 | 1 Year 24×7 FortiCare Contract (1–5100 users). |
| | FC4-10-0ACVM-248-02-12 | 1 Year 24×7 FortiCare Contract (1–10 100 users). |
| | FC8-10-0ACVM-248-02-12 | 1 Year 24×7 FortiCare Contract (1–25 100 users). |
| | FC5-10-0ACVM-248-02-12 | 1 Year 24×7 FortiCare Contract (1–50 100 users). |
| | FC6-10-0ACVM-248-02-12 | 1 Year 24×7 FortiCare Contract (1–100 100 users). |
| | FC9-10-0ACVM-248-02-12 | 1 Year 24×7 FortiCare Contract (1–500 100 users). |
| | FC7-10-0ACVM-248-02-12 | 1 Year 24×7 FortiCare Contract (1–1M users). |
| **FortiClient SSO License for FortiAuthenticator** | FCC-FAC2K-LIC | FortiAuthenticator FortiClient SSO Mobility Agent License for 2000 FortiClient connections (does not include FortiClient Endpoint Control License for FortiGate). |
| | FCC-FAC10K-LIC | FortiAuthenticator FortiClient SSO Mobility Agent License for 10 000 FortiClient connections (does not include FortiClient Endpoint Control License for FortiGate). |
| | FCC-FACUNL-LIC | FortiAuthenticator FortiClient SSO Mobility Agent License for unlimited FortiClient connections(does not include FortiClient Endpoint Control License for FortiGate). |
| **Hardware Upgrade Licenses for FAC-300F, FAC-800F, and FAC-3000F** | FAC-HW-100UG | FortiAuthenticator 300F, 800F, 3000E, or 3000F, 100 user upgrade. |
| | FAC-HW-1000UG | FortiAuthenticator 300F, 800F, 3000E, or 3000F, 1000 user upgrade. |
| | FAC-HW-10KUG | FortiAuthenticator 800F, 3000E, or 3000F, 10 000 user upgrade. |
| | FAC-HW-100KUG | FortiAuthenticator 3000F, 100 000 user upgrade. |
| **Optional Accessories** | | |
| **Power Supplies** | SP-FML900F-PS | AC power supply for FAC-300F. |
| | SP-FML900F-PS | AC power supply for FAC-800F. |

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

FORTINET

www.fortinet.com

February 3, 2025

# FortiToken™ Mobile and FortiToken™ 210

One-Time Password (OTP) Token

### Product Offerings

**FortiToken Mobile**

OATH compliant OTP generator application, supporting both time-based (TOTP) and event-based (HOTP) tokens

**FortiToken 210**

Multi-Factor Authentication, OATH compliant, TOTP. A keychain-sized device that offers real mobility and flexibility.

No client software to install. Press the button, generate and display a secure one-time password every 60 seconds. The password verifies user identity.

The LCD big screen of the rugged FortiToken 210 is easy to read. The indicator displays the time left until the next OTP generation.

## Multi-Factor Authentication Offers Real Mobility

Enable Multi-Factor Authentication with FortiToken Mobile (FTM) One-Time Password (OTP) application with push notifications or a hardware time-based OTP token. Fortinet FortiToken Mobile and hardware OTP tokens are fully integrated with FortiClient, protected by FortiGuard™, and leverage direct management and use within the FortiGate and FortiAuthenticator security platforms. Fortinet Multi-Factor Authentication solutions are easy to manage and easy to use.

## Highlights

**Available in**

Cloud

### Convenient, Strong Authentication

FortiToken is the client component of the Fortinet highly secure, simple to use and administer, and cost-effective multi-factor solution for meeting strong authentication needs. This application makes Android, iOS, and Windows mobile devices behave like a hardware-based OTP token without the hassle of having to carry yet another device. Push notification shows details on the mobile device to approve or deny with one tap.

Alternatively, hardware-based OTP tokens can be used to prevent user passwords from being stolen via phishing, dictionary, and brute-force attacks.

384629

### Ultra-Secure Token Provisioning

FortiToken Mobile is simple to use and administer and provision for the system administrator. The token seeds are generated dynamically, minimizing online exposure. Binding the token to the device is enforced and the seeds are always encrypted at rest and in motion.

### Privacy and Control

FortiToken Mobile cannot change settings on a phone, take pictures or video, record or transmit audio, or read or send emails. Further, it cannot see browser history, and it requires permission to send notifications or to change any settings.

Additionally, FortiToken Mobile cannot remotely wipe a phone. Any visibility FortiToken Mobile requires is to verify the OS version to determine app version compatibility.

While FortiToken Mobile cannot change any settings without permission, the following permissions are relevant to FortiToken Mobile operations:

- Access to camera for scanning QR codes for easy token activation
- TouchID/FaceID used for app security
- Access to the internet for communication to activate tokens and receive push notifications
- “Send Feedback by Email” to automatically populate the “Sender” field
- Internally share files between applications to prepare an attachment to be sent by email for “Send Feedback by Email”
- FortiToken must keep the phone awake while it is upgrading the internal database to avoid data corruption

## Highlights continued

### Leverages Existing Fortinet Platforms

Besides offering out-of-the-box interoperability with any time-based OATH-compliant authentication server such as FortiAuthenticator, FortiToken can also be used directly with FortiGate Next-Generation Firewalls, including with high availability configurations.

FortiGate has an integrated authentication server for validating the OTP as the second authentication factor for SSL VPN, IPsec VPN, captive portal, and administrative login. This method eliminates the need for the external RADIUS server that is typically required when implementing multi-factor solutions.

### Online Activation with FortiGuard®

FortiToken tokens can be activated online directly from FortiGate or FortiAuthenticator using the FortiGuard Center. This process maintains token seeds in a managed service repository. Once the seeds are activated, they can no longer be accessed from FortiGuard, ensuring they are safe from compromise. Alternatively, Fortinet offers an encrypted activation CD solution.

## Advantages

- Unique token provisioning service via FortiGuard minimizes provisioning overhead and ensures maximum seed security
- Perpetual token license and unlimited device transfers eliminate annual subscription fees
- Scalable solution leveraging existing end-user devices offers low entry cost and TCO
- Reduces costs and complexity by using an existing FortiGate as the Multi-Factor Authentication server
- Zero footprint solution

## Main Features

### FortiToken Mobile

- OATH time- and event-based OTP generator
- Login details pushed to phone for one-tap approval
- Mobile Application Security Certified (v3.1) for Android and iOS devices
- Patented cross platform token transfer
- PIN/Fingerprint protected application
- Copy OTP to the clipboard
- OTP time-interval display
- Serial number display
- Token and app management
- Self-erase brute-force protection
- Apple watch compatibility

### FortiToken Hardware Devices

- Integrated with FortiClient™ and protected by FortiGuard
- OATH TOTP compliant
- Large, easy-to-read, LCD display
- Long-life lithium battery
- Tamper-resistant/tamper-evident packaging
- Battery Life Indicator
- OTP Timer
- FTK-210 is FIPS 140-2 compliant

## Supported Platforms

### FortiToken Mobile

- iOS (iPhone, iPod Touch, iPad), Android, Windows
- WiFi-only devices supported (for over-the-air token activation)

### FortiToken Hardware Devices

- FortiOS 4.3 and up
- FortiAuthenticator — all versions

# Specifications

| | FORTITOKEN 210 |
|---|---|
| Time interval | 30 seconds or 60 seconds |
| Display | 6-digit high contrast LCD |
| Dimensions (Length x Width x Height) | 61.8 × 28.7 × 8.9 mm |
| Weight | 12 g |
| Operating Temperature | 50°F to 104°F (10°C to 40°C) |
| Storage Temperature | 32°F to 113°F (0°C to 45°C) |
| Water-Resistance | IP65 (Ingress Protection) |
| Casing | Hard Molded Plastic (ABS) |
| Secure Storage Medium | Static RAM |
| Battery | Lithium (non-rechargeable); minimum 3 years lifetime |
| OTP standard | OATH-TOTP (RFC6238) HMAC-SHA1 |
| Certification | RoHS, CE, FCC, ICES, UKCA |
| FIPS Certification | FIPS 140-2 Certificate |

| | FORTITOKEN MOBILE |
|---|---|
| Onboard Security Algorithm | OATH time and event based OTP generator |
| OTP Spec | RFC 6238, RFC 4226 |
| Supported Platforms | iOS (iPhone, iPod Touch, iPad, iWatch), Android, Windows 10 and Windows 11 |
| Over-the-Air Token Activation | WiFi-only devices supported |
| One-Tap Approval | Login details pushed to phone |
| PIN/Fingerprint/Facial Security | ✓ |
| Serial Number Display | ✓ |
| Token and App Management | ✓ |
| Self-Erase Brute-Force Protection | ✓ |

| PLATFORM SCALABILITY |
|---|
| FortiToken scalability for specific platforms can be found in the Fortinet Product Matrix located at http://www.fortinet.com/sites/default/files/productdatasheets/Fortinet_Product_Matrix.pdf |

## Ordering Information

| Product | SKU | Description |
|---|---|---|
| **FortiTokenMobile**<br>**Electronic license certificate** | FTM-ELIC-5 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-10 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-25 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-50 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-100 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-200 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-500 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-1000 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-2000 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-5000 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| | FTM-ELIC-10000 | Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025. |
| **FortiToken 210**<br>**Hardware Key FOB** | FTK-210-5 | Five pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request. |
| | FTK-210-20 | Twenty pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request. |
| | FTK-210-100 | One hundred pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request. |
| | FTK-210-500 | Five hundred pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request. |
| | FTK-210-1000 | One thousand pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request. |

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

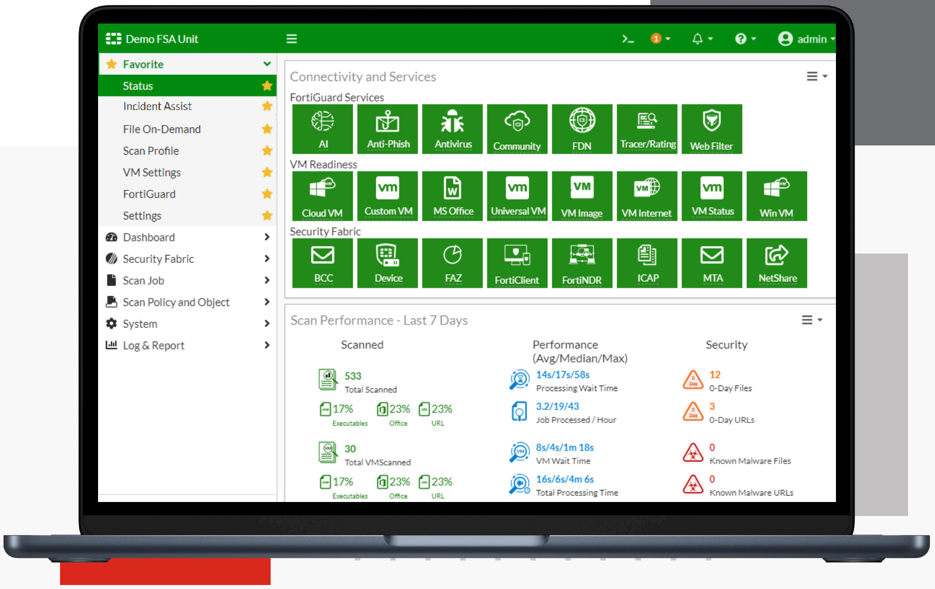
www.fortinet.com

June 3, 2025

FORTINET

Data Sheet

# FortiSandbox and FortiGuard Sandbox Services



**The new FortiSandbox is built on an advanced AI engine that defends against new, emerging, evasive, and previously unseen threats in real time.**

## Highlights

**10X Effective Throughput**
over traditional Sandboxes, allowing for ultra-scalable operations with no impact on performance

**10X Faster Real-Time Verdicts**
Accelerate incident handling, increase productivity, reduce exploit windows and reduce downtime and costs while blocking unknown files from entering the network with real-time analysis and filtering

**3X Improved Detection and Accuracy**
Detect 3X more malware accurately with near-zero false positives

**3X More Universal VMs for Scalability and Flexibility**
Choose any local, cloud, or custom virtual machine (VM) types and operating systems (OSs)

**SOC assistance**
FortiSandbox features a single pane of glass view of all threats for analysis and response to assist SOC and IR teams

## Next-Level FortiSandbox 5.0: Smarter, Faster, Scalable

FortiSandbox 5.0 is a fast and smart security solution that utilizes a combination of AI/ML, static and dynamic analysis, inline blocking, and scalable virtual environments to identify, analyze, contextualize, prioritize, and protect against advanced threats in real-time. Using an advanced AI engine running on purpose built ML, FortiSandbox 5.0 is 10X faster and offers 3X greater detection and accuracy than before with 3X more universal VMs for expansion than before to protect against malicious activity, including zero-day threats and advanced AI-powered sophisticated threats across a broad attack surface of Cloud, IT, Edge, hybrid, and OT.

FortiSandbox supports multiple operating systems and file types, and provides reporting capabilities for quick threat identification and response. Integrating natively with 12 Security Fabric products and other tools, deployable on-premises, in the cloud, or as a hosted service, FortiSandbox is suitable for organizations of any size.

## Sandboxing: a must-have in modern cyber defense

As the modern threat landscape, powered by AI enhanced threats bypass traditional defenses, sandboxing has become a critical layer in detecting the unknown and evasive —especially zero-day or fileless malware. This section highlights why sandboxing is no longer optional but an essential and foundational control in modern security strategies.

*Defend against the unknown: why sandboxing is mission-critical.*

| Framework | Region | Requirement Summary | Primary Industry or Sector |
|---|---|---|---|
| **PCI DSS v4.0** | 🌐 🇺🇸 | Mandates anti-malware and recommends advanced techniques (heuristics/ behavioral analysis). | Retail, E-commerce, Financial Services, Hospitality, Call Centers |
| **CMMC 2.0** | 🇺🇸 | Mandates malware protection. | Defense, Aerospace, Government Contractors |
| **Singapore CCoP** | ASEAN | Mandates behavior-based detection (such as sandboxing). | Critical Information Infrastructure (Energy, Water, Finance, Healthcare) |
| **EU NIS2** | 🇪🇺 | Mandates risk-based cybersecurity at national level. | Critical Infrastructure, Digital Services, Energy, Telecom |
| **NIST CSF v2.0** | 🌐 | Recommends malware detection as an outcome (such as malicious code is detected). | Critical Infrastructure, Government, Finance, Healthcare, Enterprise |
| **Japan METI/IPA** | 🇯🇵 | Recommends advanced malware detection (such as sandboxing). | Manufacturing, Technology, Energy, Critical Infrastructure |
| **EU CSA** | 🇪🇺 | May require advanced malware detection for high assurance levels and certification. | IT Products and Services (EU Market) |

Note: The industry sectors under critical infrastructure are energy, finance, health, telecommunications, transport, and water.

Sandboxing solutions like FortiSandbox offer powerful detection and protection. However, some security team members still have some doubts about the performance of sandboxing. Let’s clear the air on that.

## The truth about sandboxing speed

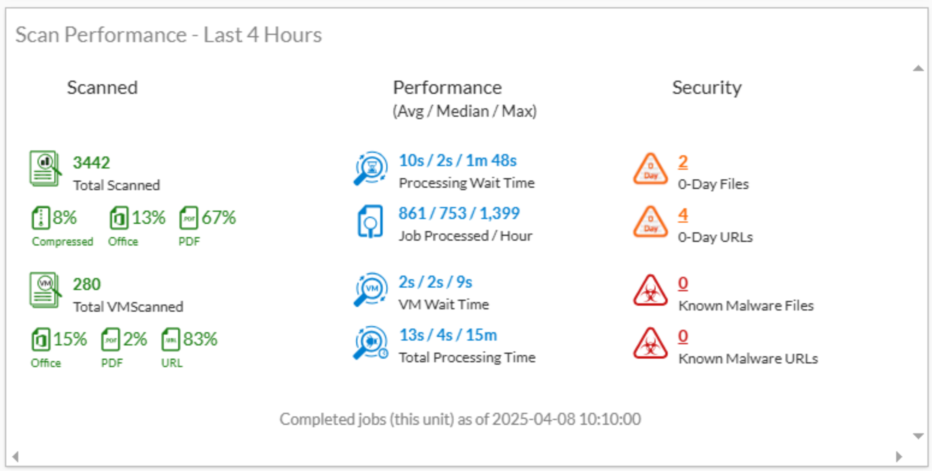
**Sandboxing isn't slow—it's smarter.**

Contrary to outdated beliefs, sandboxing doesn't have to slow things down. FortiSandbox delivers fast, AI-driven threat analysis—proving that high security and high performance can go hand in hand. One of the most common misconceptions about sandboxing is that *it's too slow for real-time protection*. In reality, FortiSandbox is **engineered for speed and efficiency** without compromising on deep threat analysis and protection. It uses a two-tiered AI-powered scanning approach—static and dynamic—to rapidly and accurately assess files.

The Static AI Scan can process up to 50 files per second, immediately identifying known malicious attributes and returning a threat verdict within milliseconds. If a file contains active content (such as embedded URLs, scripts, macros, or executables) but shows no obvious static threats, it is passed to the Dynamic AI Scan, which spins up an isolated virtual environment to detonate and observe the file's behavior—typically within a few seconds.

In a well-resourced production environment, most files are scanned in under a second, with a median scan time of just five seconds. This time-frame is well within acceptable thresholds for network, email, and endpoint solutions to safely hold files during analysis—ensuring high detection efficacy without slowing down operations.

**With speed no longer a barrier**, it's time to evaluate what really sets sandboxing solutions apart.



Scan Performance - Last 4 Hours

| Scanned | Performance<br>(Avg / Median / Max) | Security |
|---|---|---|
| 3442<br>Total Scanned | 10s / 2s / 1m 48s<br>Processing Wait Time | 2<br>0-Day Files |
| 8% Compressed<br>13% Office<br>67% PDF | 861 / 753 / 1,399<br>Job Processed / Hour | 4<br>0-Day URLs |
| 280<br>Total VMScanned | 2s / 2s / 9s<br>VM Wait Time | 0<br>Known Malware Files |
| 15% Office<br>2% PDF<br>83% URL | 13s / 4s / 15m<br>Total Processing Time | 0<br>Known Malware URLs |

Completed jobs (this unit) as of 2025-04-08 10:10:00

The screenshot illustrates the performance of FortiSandbox over the last four hours, highlighting its ability to quickly and efficiently scan a high volume of files and URLs. Over 3000 files and URLs were scanned, with only 8% (280) requiring the more time-intensive Dynamic Scan. The majority of files were processed rapidly, with a median total processing time of just 4 seconds and an average of 13 seconds. Within the efficient scanning process, a handful of suspicious detections were flagged, demonstrating the system ability to balance speed with thorough threat analysis.

## A smarter choice: feature-driven evaluation of sandbox technologies

Not all sandboxes are built the same. This section compares key capabilities that matter most—such as AI-driven analysis, deployment flexibility, integration, and automation—to help you choose the right solution for your environment.

| Advantage | FortiSandbox | Competitor | Comments |
|---|---|---|---|
| **AI/ML Capabilities** | ✓✓✓ | ✓✓ | FortiSandbox: advanced AI and ML with neural networks available on-premises and cloud, reduce latency.<br>Competitor: AI or ML engine based on cloud-based updates are slower. |
| **Zero-Day Threat Detection** | ✓✓✓ | ✓✓ | FortiSandbox: Dual analysis (static + dynamic), with fastest Sandbox database creation (e.g. 2 mins)<br>Competitor: High accuracy with rapid signature creation (e.g. 5 mins) |
| **Integration** | ✓✓✓ | ✓✓✓ | FortiSandbox: Integrates with Fortinet Security Fabric, ICAP, BCC, API.<br>Competitor: Strong integration with their ecosystem. |
| **Deployment Options** | ✓✓✓ | ✓✓ | FortiSandbox: On-prem, virtual, public-cloud and SaaS cloud.<br>Competitor: Limited selection on-prem, virtual, public-cloud or SaaS cloud. |
| **Forensics Capabilities** | ✓✓✓ | ✓✓ | FortiSandbox: Full job detailed report.<br>Competitor: Limited to moderate forensic tools. |
| **Automation and Threat Sharing** | ✓✓✓ | ✓✓✓ | FortiSandbox: Automatic signature distribution.<br>Competitor: Automatic signature distribution. |
| **Cost and Licensing** | ✓✓✓ | ✓✓ | FortiSandbox: Competitive pricing and simple licensing model.<br>Competitor: Higher tiered pricing and/or per-seat licensing. |

Once you understand the features, the next question is: how well does it work across your existing stack?

## Better and stronger together: FortiSandbox and the power of coordinated defense

FortiSandbox is designed to integrate deeply across the Fortinet Security Fabric and with third-party products to deliver advanced threat detection and automated response. Here are the most common integrations and use cases.

### 1. Next-Generation Firewall (NGFW) with Inline Blocking Option

**Use Case:** Real-time blocking of advanced threats at the network perimeter

When integrated with FortiSandbox, FortiGate NGFW becomes a proactive defense system capable of detecting and blocking sophisticated threats **before they enter the network**. It uses **Inline Scanning**, meaning files and content passing through the firewall (via HTTP, FTP, SMTP) are actively inspected **in real time**.

Suspicious files that cannot be confirmed as safe using static inspection are automatically sent to **FortiSandbox**. If the sandbox determines the file is malicious—through static or dynamic analysis—FortiGate can **immediately block the file**, quarantine the session, or take other actions, all **without delay to users or services**.

With AI-driven detection, high throughput, and tight Security Fabric integration, this setup enables **zero-day threat detection and inline prevention**, offering deep security **without the performance penalty**.

### 2. Secure Email Gateway (SEG)

**Use Case:** Prevent phishing, malware, and ransomware via email

Emails with attachments or embedded URLs are scanned through FortiSandbox **to detect hidden malware, phishing and ransomware**. If a threat is confirmed, SEG such as FortiMail can block delivery or strip dangerous content—**stopping email-borne threats before they reach inboxes**.

### 3. Endpoint Security

**Use Case:** Endpoint-level detection and response

When Endpoint Security solutions such as FortiClient or FortiEDR, encounter unknown files they forward those to FortiSandbox for analysis. If malware is detected, the endpoint agent can kill the process, isolate the host, or share IOCs with other devices—**creating a fast, coordinated response across users and systems**.

### 4. Web Proxy

**Use Case:** Block advanced web threats from downloads and scripts

Proxy devices such as FortiProxy filter web traffic and enforce policies, while FortiSandbox adds deep analysis for suspicious downloads and web content. Together, they detect and block zero-day malware, drive-by downloads, and malicious scripts—**before they ever reach the endpoint**.

### 5. Shared Storage

**Use Case**: Analyze files from SMB/NFS shares, cloud storage (e.g. OneDrive), and web uploads

FortiSandbox can scan files from shared folders and upload portals—including SMB, NFS, public shares, and cloud storage like OneDrive. By detecting hidden malware in these locations, it helps **stop lateral movement and insider threats** before they spread.

### 6. FortiAnalyzer and FortiSIEM

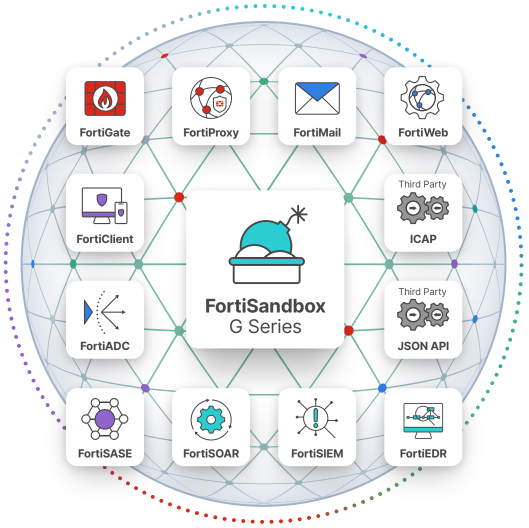
**Use Case**: Centralized visibility, correlation, and automated response

FortiSandbox shares IOCs and threat intelligence with FortiAnalyzer and FortiSIEM. These platforms correlate events, generate alerts, and trigger workflows—**accelerating detection, triage, and mitigation across the enterprise**.

### 7. Third Party Integrations (via APIs or ICAP)

**Use Case**: Extend sandboxing to external products

FortiSandbox supports **ICAP** and **RESTful APIs**, allowing integration with third-party tools like other NGFWs, proxies, SIEMs, or email gateways. This integration enables **sandbox-as-a-service** functionality even outside of Fortinet environments.



FortiSandbox doesn't work in isolation—it integrates deeply across the Fortinet Security Fabric. From firewalls and email to endpoints and storage, see how FortiSandbox delivers maximum threat coverage and protection through intelligent and coordinated defense in real-time.

Now that we've explored the value of sandboxing, addressed common misconceptions, and reviewed real-world use cases, it's time to look under the hood. The following section outlines FortiSandbox's core capabilities and technical specifications—highlighting the features that drive its speed, accuracy, and seamless integration across your security infrastructure.

## Feature Summary

FortiSandbox combines advanced threat detection with performance and flexibility, making it a powerful addition to any security stack. This section summarizes key features that define its effectiveness—from AI-driven static and dynamic analysis to flexible deployment models and seamless integration across network, endpoint, email, and cloud environments. Whether you're looking for speed, scalability, or automated response, FortiSandbox delivers where it matters most.

### Continuously Evolving AI-Powered Detection

With FortiSandbox 5.0, the Advanced AI Engine is natively integrated into the platform, combining real-time performance with purpose-built machine learning. Trained daily on thousands of newly collected malware samples across various file types, the engine adapts continuously by analyzing undetected samples and refining detection models accordingly. Each model undergoes two weeks of rigorous validation to ensure accuracy and reliability. This process enables FortiSandbox to detect, analyze, and protect against both known and unknown threats—faster and without added latency—helping organizations stay ahead of emerging attacks without the need for additional security controls or resources.

### Real-Time Phishing Detection and Prevention

The FortiSandbox provides protection against zero-day phishing. The URLs extracted from emails and embedded from documents are processed in the FortiGuard cloud. The web pages are downloaded in real-time and are analyzed using patented technologies to determine any phishing signs.

### Intelligent Threat Investigation with MITRE-Aligned Insights

FortiSandbox provides a comprehensive Job Detail Report for threat analysis and intelligence for Virtual Security Analyst. The report maps discovered malware techniques to MITRE ATT&CK framework with built-in powerful investigative tools that allow Security Operations (SecOps) teams to download captured packets, original file, tracer log, and malware screenshot. STIX 2.0 compliant IOCs provide rich threat intelligence and actionable insight after files are examined.

FortiSandbox also allows SecOps teams to optionally record a video or interact with the malware in a simulated environment.

### Flexible and Scalable Universal VM Deployment

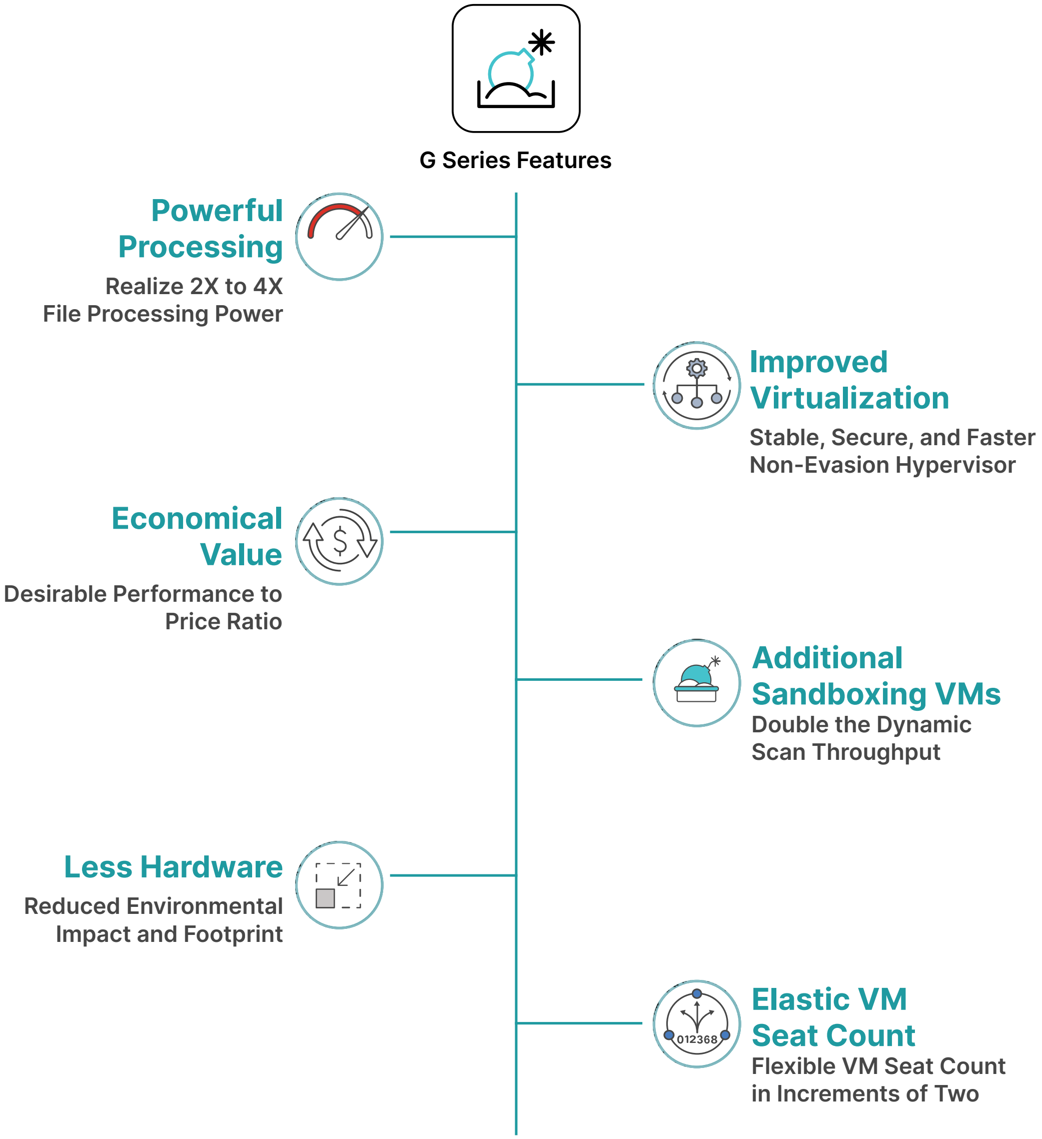
Universal VM is an all-in-one license for the flexibility to choose any local, cloud, or custom virtual machine (VM) type and operating system. It detaches VM licenses from the OS licenses to reduce licensing complexity.

### Resilient High-Availability Architecture for Continuous Protection

The FortiSandbox provides native clustering support of up to 99 worker nodes that expands throughput capacity providing uninterrupted critical operations.

## Platform Evolution

Leveraging our previous F and E models*, FortiSandbox 3000G, 1500G, and 500G provide cutting edge technological advancements, performance, real-time sharing of threat intelligence across multiple geographical locations, and integration with Fortinet's Security Fabric and third party providers. With twice the VM capacity and file processing capabilities, our G Series delivers unparalleled stability, the highest detection accuracy, and best-breed throughput, while offering flexible and cost-effective deployment solutions.



G Series Features

**Powerful Processing**
Realize 2X to 4X File Processing Power

**Improved Virtualization**
Stable, Secure, and Faster Non-Evasion Hypervisor

**Economical Value**
Desirable Performance to Price Ratio

**Additional Sandboxing VMs**
Double the Dynamic Scan Throughput

**Less Hardware**
Reduced Environmental Impact and Footprint

**Elastic VM Seat Count**
Flexible VM Seat Count in Increments of Two

*The 500G replaces the 500F, and the 1500G replaces the 1000F and 2000E.

## Detailed Summary

### Advanced Threat Protection

- Advanced AI to identify zero-day threats faster and better detection
- Inline blocking to detect and protect against Zero-day Malware including ransomware; blocks and holds malicious content at the FortiGate and sends to the sandbox for analysis/verdict
- Real-time identification of Zero-day Phishing sites including spam and malware-hosted sites
- Network threat detection in sniffer mode. Identify botnet activities and network attacks, malicious URL visits
- Threat enrichment through FortiGuard IOC
- Sandbox Community Cloud for shared analysis within the worldwide community of FortiSandbox deployments

### System Integration Support

- File and URL submission by Security Fabric devices
    - Integrated mode with FortiGate. HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM, and their equivalent SSL-encrypted versions
    - Integrated mode with FortiMail. SMTP, POP3, IMAP
    - Integrated mode with FortiClient EMS. HTTP, FTP, SMB
    - Integrated mode with FortiWeb. HTTP
- Sniffer mode. HTTP, FTP, POP3, IMAP, SMTP, SMB
- Proxy inspection via ICAP
- MTA/BCC mode via SMTP
- NetShare Scan mode via FTP, sFTP, CIFs, NFS, OneDrive, AWS S3 Buckets, Azure Blob, and Google Cloud storage.
- Dynamic Threat Intelligence DB update of malicious file checksum and URL
- JSON API to automate uploading samples and downloading actionable malware indicators to remediate
- Remote and secured logging with FortiAnalyzer, FortiSIEM, CEF servers, and syslog servers

### Deployment

- File submission from integrated device(s)
- Sniffer mode deployment with TCP RST support to reset client's connection with the suspicious server
- Network Share Scan with large file support (e.g., ISO images, network shared folders, SMB/NFS, AWS S3, and Azure Blob)
- Proxy adapter submission with multi-tenancy support
- OT deployment with supported services: BACnet, HTTP, IPMI, Modbus, S7comm, SNMP, TFTP
- High-availability with Primary and Secondary nodes for redundancy
- Port monitoring for cluster fail-over
- Clustering up to 99 worker nodes for higher throughput
- Air-gapped networks support
- Aggregate interface support for increased bandwidth and redundancy
- Isolated administrative traffic from VM image traffic

## Detailed Summary continued

### Advanced AI Scan (Static AI Scan) Features

- Integrated with the new Advanced AI engine and model
- Integrated with the full FortiGuard Antivirus database of heuristic and checksum signatures
- Intelligent adaptive scan profile that optimizes sandbox resources based on submissions
- Parallel scan to run multiple distinct VM types simultaneously
- Extracts and scan files embedded in documents
- Extracts and scan URLs embedded in documents and QR Code
- Extracts and scan images in documents using OCR
- Integrate with third-party Yara rules
- Cloud query for latest known Malware and clean files
- File checksum whitelist and blacklist options
- Scan URLs from submitted emails and files
- Rating Engine Plus that leverages the latest FortiGuard ML rating
- VM scan ratio for efficient utilization of VMs

### Sandboxing VM (Dynamic AI Scan) Support

- AI-powered behavioral analysis constantly learning new malware and ransomware techniques
- Concurrent dynamic analysis VM instances
- OS type supported: Windows 11/10/8.1/7, macOS, Linux, Android, and ICS systems
- Customizable VMs for Windows and Linux OS
- Configurable internet browser supporting Internet Explorer, Microsoft Edge, Google Chrome, and Mozilla Firefox
- Sandbox interactive mode, video-recording of malware interaction and VM screenshots
- Nested VMs on premise and cloud deployment
- Anti-evasion detection techniques
  - API Obfuscation
  - Bare-metal Detection
  - Command and Control
  - Direct System Calls
  - Execution Delay
  - Memory Only Payload
  - Process Hollowing/Injection
  - Runtime Encryption/Packing
  - System Fingerprinting
  - Time Bomb
  - User Files Check
  - User Interaction Check
  - VM/Sandbox Detection
- Callback detection. Malicious URL visit, botnet C&C communication, and attacker traffic from activated malware
- Downloadable captured packets, tracer logs, and screenshots
- File Types Support: Windows Executable, Microsoft Office, Document/Email, Android files, Linux files, MacOS, Web files
- File Compression Support
- User-defined extensions

## Detailed Summary continued

### Monitoring and Reporting

- AI-based Threat Summary using the collected indicators and results
- Dashboard widgets for connectivity and services, license status, scan performance, system resources
- Scan performance page for tracking historical usage
- Real-time monitoring widgets. Scanning result statistics, scanning activities (over time), top targeted hosts, top malware, top infectious URLs, top callback domains
- Drilldown event viewer. Dynamic table including actions, malware name, rating, type, source, destination, detection time, and download path
- Reports and logging. GUI, download PDF, and raw log file
- Detailed Job Report generation
- Periodic logs of system status, performance, scan statistics, and system resource usage
- MITRE ATT&CK v11 support
- Download tracer logs, PCAP, and indicators in STIX 2.0 format
- Notification emails when a malicious file is detected
- Weekly reports to global email lists and administrators
- TAC-report for comprehensive snapshot of system configuration and status

### Administration

- Configuration via GUI and CLI
- Multiple administrator accounts supporting full or view only access
- Radius authentication for administrators
- Single Sign-On via SAML
- Self-Check widget for configurations, connectivity, and services
- Cluster management page for administering the HA and cluster nodes
- Centralized search page allowing administrators to build customized search conditions
- Upload any license from a single convenient page
- VM status monitoring
- Automatic engine and signature updates
- Automatic check for new VM image availability
- System health check alerting system
- NTP via FortiGuard support
- Backup, restore, and revision of system configuration
- Consolidated CLI for troubleshooting
- Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
- Option on NetShare scan mode to prioritize and forward files to a third-party scanning for further scanning

# Deployment and Detection Specifications

| FEATURE | CLOUD | | | | ON PREMISE | |
|---|---|---|---|---|---|---|
| | FSA SaaS | FSA IL MPS | FSA PaaS | FSA Public Cloud | FSA VMs | FSA Hardware |
| **Deployment and Integration** | | | | | | |
| **Type** | | | | | | |
| Deployment | Fortinet Hosted | Fortinet Hosted | Fortinet Hosted | Azure, AWS, GCP, OCI | On Premise | On Premise |
| Hosting | Shared | Shared | Dedicated | Dedicated | Dedicated | Dedicated |
| **Integration** | | | | | | |
| Security Fabric | Centralized | Centralized | Centralized | Centralized | Centralized | Centralized |
| Fabric Partner | — | — | ✓ | ✓ | ✓ | ✓ |
| API, BCC, ICAP, MTA, NetShare, and Sniffer Mode | — | — | only API | ✓ | ✓ | ✓ |
| **FortiGate Capabilities** | | | | | | |
| Detection (Visibility and Log Enrichment) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Prevention (Inline Blocking) | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Detection** | | | | | | |
| **Static Analysis** | | | | | | |
| Advanced AI[1] | ✓ | ✓ | Coming Q4 2025 | ✓[1] | ✓[1] | ✓[1] |
| Static AI Engine[3] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Accelerated AI Pre-filter[2] | | ✓ | Add-on | Add-on | Add-on | Add-on |
| Antivirus Extended DB | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Web Filtering | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Dynamic Analysis** | | | | | | |
| Dynamic AI Engine[3] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Analysis Time | up to 60 mins | 1-5 minutes | 1-3 minutes | 1-3 minutes | 1-3 minutes | 1-3 minutes |
| Universal VM[4] | | | | ✓ | ✓ | ✓ |
| Real-Time Anti-Phishing | | | Add-on | ✓[1] | ✓[1] | ✓[1] |
| Anti-Evasion Detection | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| IPS and C&C Detection | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Supported OS** | | | | | | |
| Windows | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| MacOS, Linux, Android | — | ✓[5] | ✓[5] | ✓ | ✓ | ✓ |
| Custom VM | — | — | — | ✓ | ✓ | ✓ |
| OT Simulation | — | — | — | ✓ | ✓ | ✓ |

1. Available as part of "Advanced Sandbox Threat Intelligence" subscription running on firmware version 5.0.
2. Add-on integration with FortiNDR appliance for fast pre-filtering.
3. AI-powered content and behavioral analysis through Machine Learning Model updated via Sandbox Threat Intelligence subscription.
4. Supported on firmware version 5.0.
5. Dynamic Scan on Android is scheduled for 2025/Q3.

## Supported File Type Specifications

| FEATURE | CLOUD | | | | ON PREMISE | |
|---|---|---|---|---|---|---|
| | FSA SaaS | FSA IL MPS | FSA PaaS | FSA Public Cloud | FSA VMs | FSA Hardware |
| **Supported File Type** | | | | | | |
| **Windows Executables** | | | | | | |
| Portable executable (exe, dll, scr) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Installer and script files (bat, cmd, jse, msi, ps1, vbe, vbs, wsf) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Productivity Files** | | | | | | |
| Microsoft Office (Word, Excel, Powerpoint, Publisher, OneNote) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Portable document format files (pdf) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Other related files (csv, ics, rtf) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Email** | | | | | | |
| Email files (eml, msg) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Links contained in emails (lnk) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Web files** | | | | | | |
| Common files (html, js, lnk, url) | — | — | ✓ | ✓ | ✓ | ✓ |
| Adobe Flash files (swf) | — | — | ✓ | ✓ | ✓ | ✓ |
| **Images** | | | | | | |
| Images with QR Code and Ransomware | — | — | ✓ | ✓ | ✓ | ✓ |
| **Additional OS** | | | | | | |
| Android application package files (apk) | — | ✓[1] | ✓[1] | ✓ | ✓ | ✓ |
| Linux and Shell scripts files (elf, sh) | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| MacOS files (dmg) | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Archive Common files** | | | | | | |
| Common files (7z, arj, cab, bzip, gzip, jar, lzw, rar, tar, lzh, zip, xz) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Additional Archive files (ace, iso, kgb, pst, tgz, udf, upx, vhd, z) | — | — | ✓ | ✓ | ✓ | ✓ |

[1] Dynamic Scan on Android is scheduled for 2025/Q3.

# Capacity and Performance Specifications

| FEATURE | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | FSA-PaaS | FSA-VMS1 | FSA-VMS2 | FSA-VMS3 | FSA-VMS4[9] | FSA-500G | FSA-1500G | FSA-3000G |
| **Capacity** | | | | | | | | |
| Local VM Capacity | | 0-8 | 0-16 | 0-32 | 0-64 | 2-14 | 2-28 | 8-150 |
| Cloud VM Expansion[1] | 1-200 | 1-200 | 1-200 | 1-200 | 1-200 | 1-80 | 1-120 | 1-200 |
| **Performance and Capacity** | | | | | | | | |
| Effective Sandboxing Throughput[2] (Files/Hr) | 5000[3] | 8000[4] | 24 000 | 48 000 | 96 000 | 10 000 | 32 000 | 160 000 |
| Static Analysis Throughput[5] (Files/Hr) | 10 000[3] | 20 000[4] | 60 000 | 120 000 | 240 000 | 20 000 | 80 000 | 320 000 |
| Dynamic Analysis Throughput[6] (Files/Hr) | 160[3] | 200[4] | 400 | 800 | — | 500 | 1000 | 5700 |
| FortiMail Throughput[7] (Emails/Hr) | 50 000 | 80 000 | 240 000 | 480 000 | 960 000 | 100 000 | 320 000 | 1 600 000 |
| MTA Adapter Throughput (Emails/Hr) | — | 20 000 | 60 000 | 120 000 | 240 000 | 25 000 | 80 000 | 320 000 |
| Sniffer Mode Throughput (Gbps) | — | 1 | TBD | TBD | TBD | 0.5 | 4 | 9.6 |
| Number of Users[8] | 650 | 1000 | 3000 | 6000 | 12 000 | 1250 | 4000 | 20 000 |

Notes:

The FSA VMS is tested on premise Hyper-V server with corresponding CPUs, memory, and VMs.

The FSA Public Cloud BYOL could achieve similar performance based on chosen resources.

The performance of FSA SaaS, FSA IL MPS and FSA Public Cloud PAYG are not included, as they cannot be accurately measured.

1. The ranges reflect Universal VM support through firmware version 5.0.
2. Tested based on files with 80% documents and 20% executables; measured based on v5.0. Includes both static and dynamic analysis with pre-filtering enabled.
3. Tested on default Flavor-1 VM (with 4 CPUs and 8GB RAM) and 8 VMs. A higher VM flavor can be provided with 20 or more VM subscriptions for higher capacity. To inquire about VM flavors contact your account representative.
4. Tested on a Hyper-V (with 16 CPUs and 32GB RAM) and 8 VMs.
5. Includes receiving, job handling, AV engine, Yara engine, Cloud Query; measured based on v5.0.
6. Tested with Static Analysis and all files are forwarded to Dynamic Analysis.
7. Based on a ratio of one email with attachment to 10 emails.
8. Based on a ratio of one user per 80 emails on 10 hour period with 10% on Dynamic Scan.
9. Throughput is constrained by the 96 vCPU limit in version 5.0.

# Hardware Specifications

| FEATURE | | | |
|---|---|---|---|
| | FSA 500G | FSA 1500G | FSA 3000G |
| System Information | | | |
| Form Factor | 1RU Appliance | 1RU Appliance | 2RU Appliance |
| Network Interfaces | 4x GE RJ45 ports | 4x GE RJ45 ports, 2× 10 GE SFP+ slots | 8× 10 GE SFP+ slots |
| Storage | 1× 960 GB | 2× 960 GB RAID1 | 4× 2 TB RAID-10 |
| Hot Swappable | — | ✓ | ✓ |
| Trusted Platform Module (TPM) | ✓ | ✓ | ✓ |
| Dimensions | | | |
| Height x Width x Length (inches) | 1.73×17.24×14.96 | 1.73×17.24×24.02 | 3.5×17.2×25.6 |
| Height x Width x Length (mm) | 44×438×380 | 44×438×610 | 88×438×650 |
| Weight (lbs/kg) | 11.42 lbs (5.18 kg) | 24.92 lbs (11.30 kg) | 44 lbs (20 kg) |
| Power | | | |
| Number of Power Supplies | 1x | 2x | 2x |
| Power Supply (AC/DC) | 100–240V AC 50/60 Hz | 100–240V AC, 50/60 Hz | 100–240V AC, 50/60 Hz |
| Maximum Current (AC/DC) | 100V/6A, 240V/3A | 100V/7.5A, 240V/3.9A | 100V/10A, 240V/5A |
| Power Consumption (Average/Maximum) | 71.8 W / 87.8 W | 238.1 W / 291.06 W | 471.9 W / 542.4 W |
| Redundancy | — | ✓ | ✓ |
| Hot Swappable | — | ✓ | ✓ |
| Environment | | | |
| Forced Airflow | Front to Back | Front to Back | Front to Back |
| Heat Dissipation | 333.63 BTU/h | 1027.22 BTU/h | 1850.67 BTU/h |
| Operating Temperature | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) |
| Storage Temperature | -40°F to 158°F (-40°C to 70°C) | -40°F to 158°F (-20°C to 70°C) | -40°F to 158°F (-40°C to 70°C) |
| Humidity | 10% to 90% non-condensing | 10% to 90% non-condensing | 10% to 90% (non-condensing) |
| Compliance | | | |
| Certifications | FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST | | |
| Additional Services | | | |
| 24 × 7 Support | ✓ | ✓ | ✓ |

FortiSandbox 500G

FortiSandbox 1500G

FortiSandbox 3000G

## Integration Matrix

| | CLOUD | | | | APPLIANCES |
|---|---|---|---|---|---|
| **Product** | **SaaS** | **Inline Sandbox** | **FortiSandbox Cloud (PaaS)** | **Private/Public Cloud** | **VM / Hardware** |
| **FORTIGATE** | FortiOS V7.0+ | FortiOS V7.2.1+,<br>FortiOS V7.4.1+ (PaaS) | FortiOS V7.0+ | FortiOS V7.0+ | |
| **FORTICLIENT** | FortiClient for Windows OS V7.0+ | | FortiClient for Windows OS V7.0+ | FortiClient for Windows OS V7.0+ | |
| **FORTIMAIL** | FortiMail OS V6.2+ | | FortiMail V7.0+ | FortiMail OS V7.0+ | |
| **FORTIWEB** | FortiWeb OS V7.0+ | | | FortiWeb OS V7.0+ | |
| **FORTIADC** | FortiADC OS v6.0+ | | | FortiADC OS V7.0+ | |
| **FORTIPROXY** | FortiProxy OS v7.0+<br>FortiProxy OS v7.4+ | | | FortiProxy OS V7.0+ | |

## Ordering Information

The following SKU list outlines the primary Sandbox deployment options. For full guidance, please refer to the related ordering guides at https://www.fortinet.com/resources/ordering-guides.

| Product | SKU | Description |
|---|---|---|
| **FortiSandbox SaaS for FortiGate** | | |
| **Enterprise Protection (includes IL MPS) (FGT-60F)** | FC-10-0060F-809-02-DD | Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium). |
| **Inline Malware Prevention Service (IL MPS) (a la carte SKU) (FGT-60F)** | FC-10-0060F-577-02-DD | FortiGuard AI-based Inline Malware Prevention Service. (Also available as part of the Enterprise Bundle). |
| **Cloud Sandbox (FGT-60F)** | FC-10-0060F-100-02-DD | Advanced Malware Protection (AMP) Bundle including Antivirus, Mobile Malware and FortiGate Cloud Sandbox Service. |
| **FortiSandbox SaaS for Security Fabric** | | |
| **Cloud Sandbox for FortiMail (FML-200F)** | FC-10-FE2HF-123-02-DD | FortiMail Cloud Sandbox - Cloud Sandbox for FortiMail. |
| **Cloud Sandbox for FortiWeb (FWB-100E)** | FC-10-W01HE-123-02-DD | FortiWeb Cloud Sandbox - Cloud Sandbox for FortiWeb. |
| **Cloud Sandbox for FortiProxy (FPX-400E)** | FC1-10-XY400-514-02-DD | SWG Protection Bundle which includes Sandbox Cloud. |
| **Cloud Sandbox for FortiADC (FAD-220F)** | FC-10-AD2AF-123-02-DD | FortiADC Cloud Sandbox - Cloud Sandbox for FortiADC. |
| **FortiSandbox PaaS** | | |
| **FortiSandbox Cloud 1 VM** | FC1-10-SACLP-433-01-DD | Cloud VM Service for FortiSandbox Cloud. Expands Cloud VM for Windows/macOS/Linux/Android by one. (Maximum of 200 VMs per FortiSandbox. |
| **FortiSandbox Cloud 5 VMs** | FC2-10-SACLP-433-01-DD | Cloud VM Service for FortiSandbox Cloud. Expands Cloud VMs for Windows/MacOS/Linux/Android by five. (Maximum of 200 VMs per FortiSandbox. |
| **FortiSandbox Pub Cloud / FortiSandbox VM Appliance** | | |
| **FortiSandbox-VMS** | FSA-VMS | Subscription license for FortiSandbox-VM with Advanced AI bundle, supporting 16 vCPUs and expandable up to 8 Universal VMs. |
| **FortiSandbox On Premise Hardware** | | |
| **FortiSandbox 500G** | FSA-500G | Sandboxing Hardware Appliance for SMB. Includes two Universal VM count. Available VM count expansion up to max 14 Local and 80 Cloud. Includes 1xWin11, 1xWin10, 1xOffice21 Licenses. |
| **FortiSandbox 1500G** | FSA-1500G | Sandboxing Hardware Appliance for Mid-Range. Includes two Universal VM count. Available VM count expansion up to max 28 Local and 120 Cloud. Includes 1xWin11, 1xWin10, 1xOffice21 Licenses. |
| **FortiSandbox 3000G** | FSA-3000G | Sandboxing Hardware Appliance for Enterprise. Includes eight Universal VM count. Available VM count expansion up to max 150 Local and 200 Cloud. Includes 4xWin10, 4xWin11, 1xOffice21 Licenses. |

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

August 27, 2025