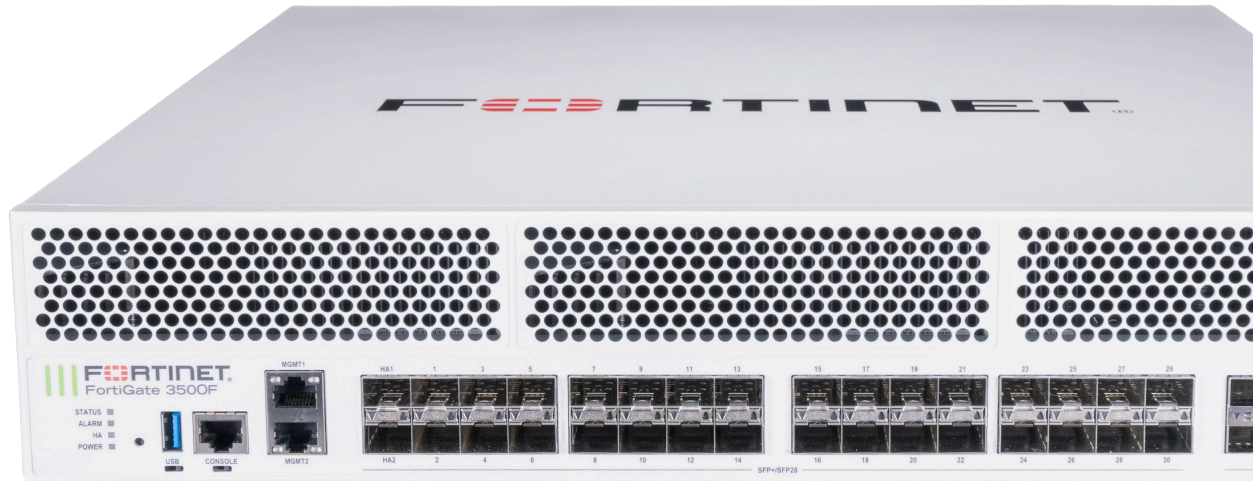


FortiGate 3500F Series

FG-3500F and FG-3501F



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

Security-Driven Networking FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented / SPU / vSPU processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Hyperscale Security to secure any edge at any scale.

High Performance with Flexibility

The FortiGate 3500F Series enables organizations to build security-driven networks that can weave security deep into their datacenter and across their hybrid IT architecture to protect any edge at any scale.

Powered by a rich set of AI/ML-based FortiGuard Services and an integrated security fabric platform, the FortiGate 3500F Series delivers coordinated, automated, end-to-end threat protection across all use cases.

The industry's first integrated Zero Trust Network Access (ZTNA) enforcement within an NGFW solution, FortiGate 3500F automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

| IPS | NGFW | Threat Protection | Interfaces |
|---------|---------|-------------------|---|
| 72 Gbps | 65 Gbps | 63 Gbps | Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 100 GE QSFP28 / 40 GE QSFP+ slots |



Available in



Appliance



Virtual



Hosted



Cloud



Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

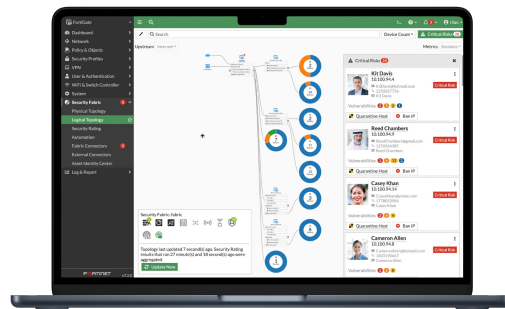
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

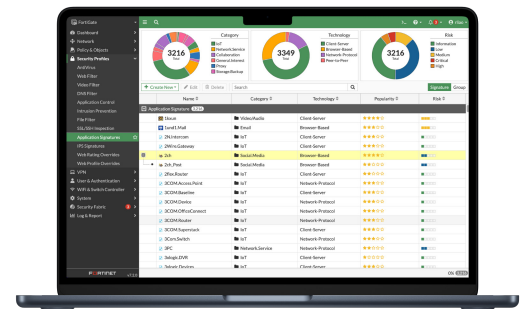
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations



Intuitive easy to use view into the network and endpoint vulnerabilities

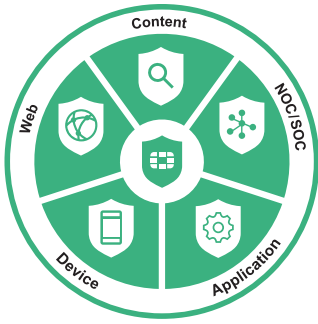


Visibility with FOS Application Signatures

FortiConverter Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. 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.





FortiGuard Services

FortiGuard AI-Powered Security

FortiGuard's rich suite of security services counter threats in real time using AI-powered, coordinated protection designed by FortiGuard Labs security threat researchers, engineers, and forensic specialists.

Web Security

Advanced cloud-delivered URL, DNS (Domain Name System), and Video Filtering providing complete protection for phishing and other web born attacks while meeting compliance.

Additionally, its dynamic inline CASB (Cloud Access Security Broker) service is focused on securing business SaaS data, while inline ZTNA traffic inspection and ZTNA posture check provide per-sessions access control to applications. It also integrates with the FortiClient Fabric Agent to extend protection to remote and mobile users.

Content Security

Advanced content security technologies enable the detection and prevention of known and unknown threats and file-based attack tactics in real-time. With capabilities like CPRL (Compact Pattern Recognition Language), AV, inline Sandbox, and lateral movement protection make it a complete solution to address ransomware, malware, and credential-based attacks.

Device Security

Advanced security technologies are optimized to monitor and protect IT, IIoT, and OT (Operational Technology) devices against vulnerability and device-based attack tactics. Its validated near-real-time IPS intelligence detects, and blocks known and zero-day threats, provides deep visibility and control into ICS/OT/SCADA protocols, and provides automated discovery, segmentation, and pattern identification-based policies.

Advanced Tools for SOC/NOC

Advanced NOC and SOC management tools attached to your NGFW provide simplified and faster time-to-activation.

SOC-as-a-Service

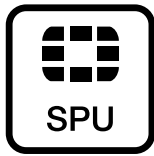
Includes tier-one hunting and automation, log location, 24x7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

Fabric Rating Security Best Practices

Includes supply chain virtual patching, up-to-date risk and vulnerability data to deliver quicker business decisions, and remediation for data breach situations.



Secure Any Edge at Any Scale



Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage



Network Processor 7 NP7

Network Processors operate inline to deliver unmatched performance and scalability for critical network functions. Fortinet's breakthrough SPU NP7 network processor works in line with FortiOS functions to deliver:

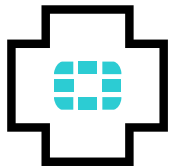
- Hyperscale firewall, accelerated session setup, and ultra-low latency
- Industry-leading performance for VPN, VXLAN termination, hardware logging, and elephant flows



Content Processor 9 CP9

Content Processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and 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, and accelerated antivirus processing



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.



Use Cases



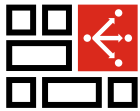
Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated 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 (Security Processing Unit) technology provides industry-leading high-performance protection



Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security—from the branch to the datacenter 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



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 work-from-anywhere models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing



HyperScale

- Purpose-built SPUs power FortiOS to consolidate networking and security and deliver ultra-scalable Security-Driven Networks
- Unparalleled ultra-high performance offers the industry's highest number of connections and connections per second performance combined with security-enabled performance to safeguard business-critical applications
- Hardware assisted anti-DDoS prevents volumetric attacks and delivers strong security posture

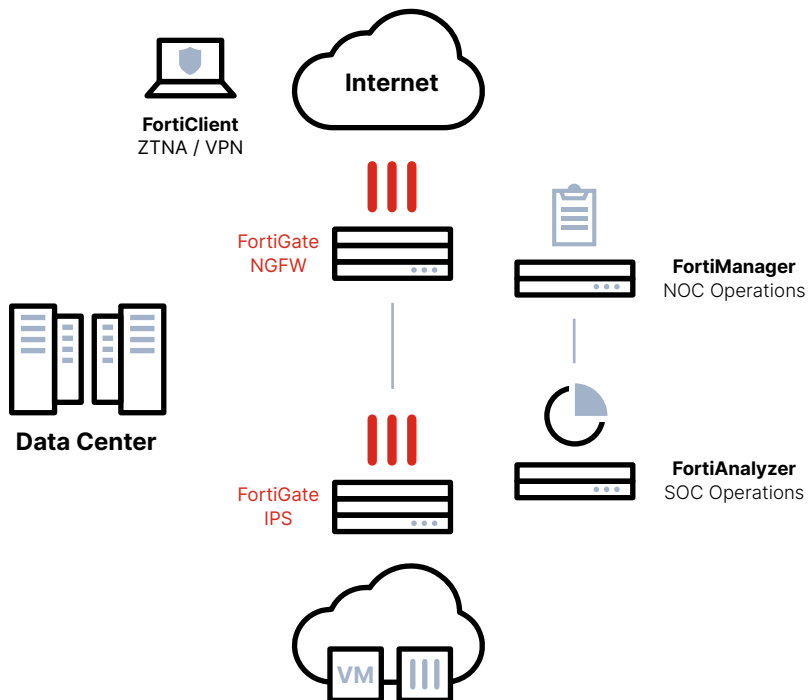




Mobile Security for 4G, 5G, and IoT

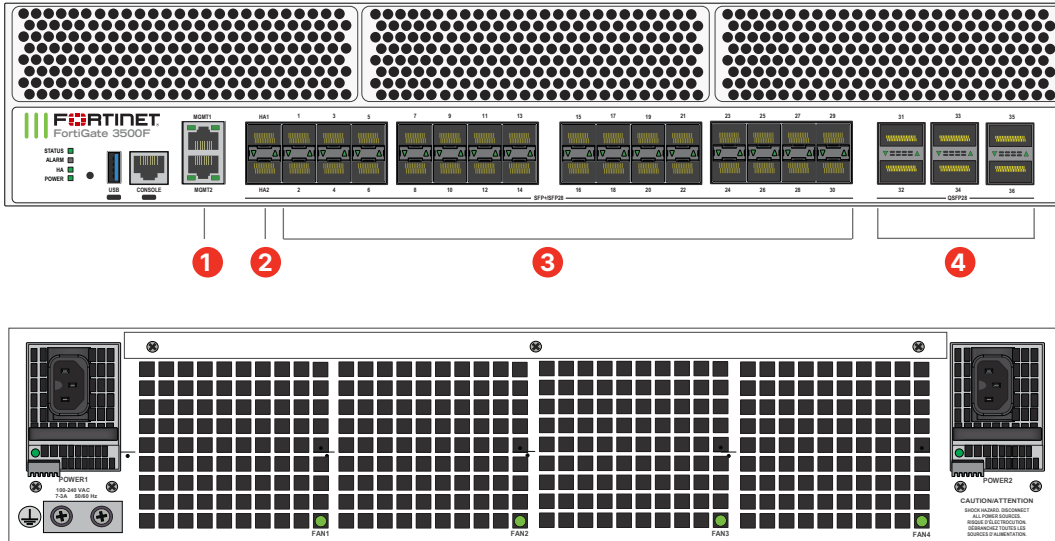
- SPU-accelerated, high performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/ DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- RAN Access Security with highly scalable and highest-performing IPsec aggregation and control Security Gateway (SecGW)
- User plane security enabled by full threat protection and visibility into GTP-U inspection

Datacenter Deployment (NGFW, IPS, Segmentation)



Hardware

FortiGate 3500F Series



Interfaces

1. 2 × 10 GE / GE RJ45 Management Ports
2. 2 × 25 GE SFP28 / 10 GE SFP+ HA Slots
3. 30 × 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
4. 6 × 100 GE QSFP28 / 40 GE QSFP+ Slots

Hardware Features



Hyperscale Firewall License

This perpetual license empowers organizations by unlocking further performance boosts. The Hyperscale Firewall License enables the hardware acceleration of CGNAT features by utilizing Fortinet's patented SPU NP7. These features include hardware session setup, firewall session logging, and NAT.

Trusted Platform Module (TPM)

The FortiGate 3500F 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.



Specifications

| | FG-3500F | FG-3501F |
|--|----------|---|
| Interfaces and Modules | | |
| Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots | | 6 |
| Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots | | 32 |
| 10GE/ GE RJ45 Management Ports | | 2 |
| USB Ports (Client / Server) | | 1 / 1 |
| Console Port | | 1 |
| Onboard Storage | — | 2× 2TB SSD |
| Trusted Platform Module (TPM) | | Yes |
| Included Transceivers | | 2x SFP+ (SR 10 GE) |
| System Performance — Enterprise Traffic Mix | | |
| IPS Throughput ² | | 72 Gbps |
| NGFW Throughput ^{2,4} | | 65 Gbps |
| Threat Protection Throughput ^{2,5} | | 63 Gbps |
| System Performance and Capacity | | |
| IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) | | 595 / 590 / 420 Gbps |
| IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) | | 595 / 590 / 420 Gbps |
| Firewall Latency (64 byte, UDP) | | 2.98 µs |
| Firewall Throughput (Packet per Second) | | 630 Mpps |
| Concurrent Sessions (TCP) | | 140 Million / 348 Million* |
| New Sessions/Second (TCP) | | 1 Million / 5 Million* |
| Firewall Policies | | 200 000 |
| IPsec VPN Throughput (512 byte) ¹ | | 165 Gbps |
| Gateway-to-Gateway IPsec VPN Tunnels | | 40 000 |
| Client-to-Gateway IPsec VPN Tunnels | | 200 000 |
| SSL-VPN Throughput ⁶ | | 16 Gbps |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | | 30 000 |
| SSL Inspection Throughput (IPS, avg. HTTPS) ³ | | 63 Gbps |
| SSL Inspection CPS (IPS, avg. HTTPS) ³ | | 60 000 |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³ | | 15 Million |
| Application Control Throughput (HTTP 64K) ² | | 135 Gbps |
| CAPWAP Throughput (HTTP 64K) | | 65 Gbps |
| Virtual Domains (Default / Maximum) | | 10 / 500 |
| Maximum Number of FortiSwitches Supported | | 300 |
| Maximum Number of FortiAPs (Total / Tunnel) | | 4096 / 2048 |
| Maximum Number of FortiTokens | | 20 000 |
| High Availability Configurations | | Active-Active, Active-Passive, Clustering |

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.



| | FG-3500F | FG-3501F |
|---|---|--------------------|
| Dimensions and Power | | |
| Height x Width x Length (inches) | 3.5 × 17.4 × 21.9 | |
| Height x Width x Length (mm) | 89 × 443 × 556 | |
| Weight | 43.8 lbs (19.9 kg) | 45.3 lbs (20.6 kg) |
| Form Factor (supports EIA/non-EIA standards) | Rack Mount, 2 RU | |
| AC Power Supply | 100–240V AC, 50/60 Hz | |
| Power Consumption (Average / Maximum) | 760 W / 1174 W | 765 W / 1181 W |
| AC Current (Maximum) | 12A@120V, 9A@240V | |
| Heat Dissipation | 4006 BTU/h | 4030 BTU/h |
| Redundant Power Supplies (Hot Swappable) | Yes (Default dual AC PSU for 1+1 Redundancy) | |
| Power Supply Efficiency Rating | 80Plus Compliant | |
| Operating Environment and Certifications | | |
| Operating Temperature | 32°–104°F (0°–40°C) | |
| Storage Temperature | -31°–158°F (-35°–70°C) | |
| Humidity | 20%–90% non-condensing | |
| Noise Level | 53.5 dBA | |
| Forced Airflow | Front to Back | |
| Operating Altitude | Up to 10 000 ft (3048 m) | |
| Compliance | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB | |
| Certifications | USGv6/IPv6 | |

*Requires Hyperscale Firewall License

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.

Ordering Information

| Product | SKU | Description |
|--|----------------------|---|
| FortiGate 3500F | FG-3500F | 6× 100GE/ 40GE QSFP28 slots and 32× 25GE/ 10GE SFP28 slots, 2× 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, and 2 AC power supplies. |
| FortiGate 3501F | FG-3501F | 6× 100GE/ 40GE QSFP28 slots and 32× 25GE/ 10GE SFP28 slots, 2× 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 4 TB SSD onboard storage, and 2 AC power supplies. |
| Optional Accessories/Spares | SKU | Description |
| Rack Mount Sliding Rails | SP-FG3040B-RAIL | Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D/DC, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC. |
| AC Power Supply | FG-7040E-PS-AC | 1500W AC Power Supply for FG-3500F, FG-3501F, FG-3700F, FG-3701F, FG-7030E, FG-7040E, FG-6000F, and FG-3900E series (not compatible for use with FG-7060E), does not include SP-FGPCORC15-XX power cord. |
| 1 GE SFP LX Transceiver Module | FN-TRAN-LX | 1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GE SFP RJ45 Transceiver Module | FN-TRAN-GC | 1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GE SFP SX Transceiver Module | FN-TRAN-SX | 1 GE SFP SX 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+ Active Direct Attach Cable, 10m / 32.8 ft | SP-CABLE-ADASFP+ | 10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots. |
| 25 GE SFP28 Transceiver Module, Short Range | FN-TRAN-SFP28-SR | 25 GE SFP28 transceiver module, short range for all systems with SFP28 slots. |
| 25 GE SFP28 Transceiver Module, Long Range | FG-TRAN-SFP28-LR | 25 GE SFP28 transceiver module, long range for all systems with SFP28 slots. |
| 40 GE QSFP+ Transceiver Module, Short Range | FN-TRAN-QSFP+SR | 40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots. |
| 40 GE QSFP+ Transceiver Module, Short Range BiDi | FG-TRAN-QSFP+SR-BIDI | 40 GE QSFP+ transceiver module, short range BiDi for all systems with QSFP+ slots. |
| 40 GE QSFP+ Transceiver Module, Long Range | FN-TRAN-QSFP+LR | 40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots. |
| 100 GE QSFP28 Transceivers, Short Range | FN-TRAN-QSFP28-SR | 100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots. |
| 100 GE QSFP28 Transceivers, Long Range | FN-TRAN-QSFP28-LR | 100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots. |
| 100 GE QSFP28 Transceivers, CWDM4 | FN-TRAN-QSFP28-CWDM4 | 100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots. |



Subscriptions

| Service Category | Service Offering | A-la-carte | Bundles | | |
|--------------------------------------|---|------------|-----------------------|---------------------------|--------------------------------------|
| | | | Enterprise Protection | Unified Threat Protection | Advanced Threat Protection |
| Security Services | FortiGuard IPS Service | • | • | • | • |
| | FortiGuard Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service | • | • | • | • |
| | FortiGuard Web Security — URL and web content, Video and Secure DNS Filtering | • | • | • | |
| | FortiGuard Anti-Spam | | • | • | |
| | FortiGuard IoT Detection Service | • | • | | |
| | FortiGuard Industrial Security Service | • | • | | |
| | FortiCloud AI-based Inline Sandbox Service ¹ | • | | | |
| NOC Services | FortiGate Cloud (SMB Logging + Cloud Management) | • | | | |
| | FortiGuard Security Fabric Rating & Compliance Monitoring Service | • | • | | |
| | FortiConverter Service | • | • | | |
| | FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service | • | | | |
| SOC Services | FortiAnalyzer Cloud | • | | | |
| | FortiAnalyzer Cloud with SOCaaS | • | | | |
| Hardware and Software Support | FortiCare Essentials | • | | | |
| | FortiCare Premium | • | • | • | • |
| | FortiCare Elite | • | | | |
| Base Services | FortiGuard Application Control | | | | |
| | FortiCloud ZTNA Inline CASB Service ¹ | | | | |
| | Internet Service (SaaS) DB Updates | | | | |
| | GeolP DB Updates | | | | included with FortiCare Subscription |
| | Device/OS Detection Signatures | | | | |
| | Trusted Certificate DB Updates | | | | |
| | DDNS (v4/v6) Service | | | | |

1. Available when running FortiOS 7.2



FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

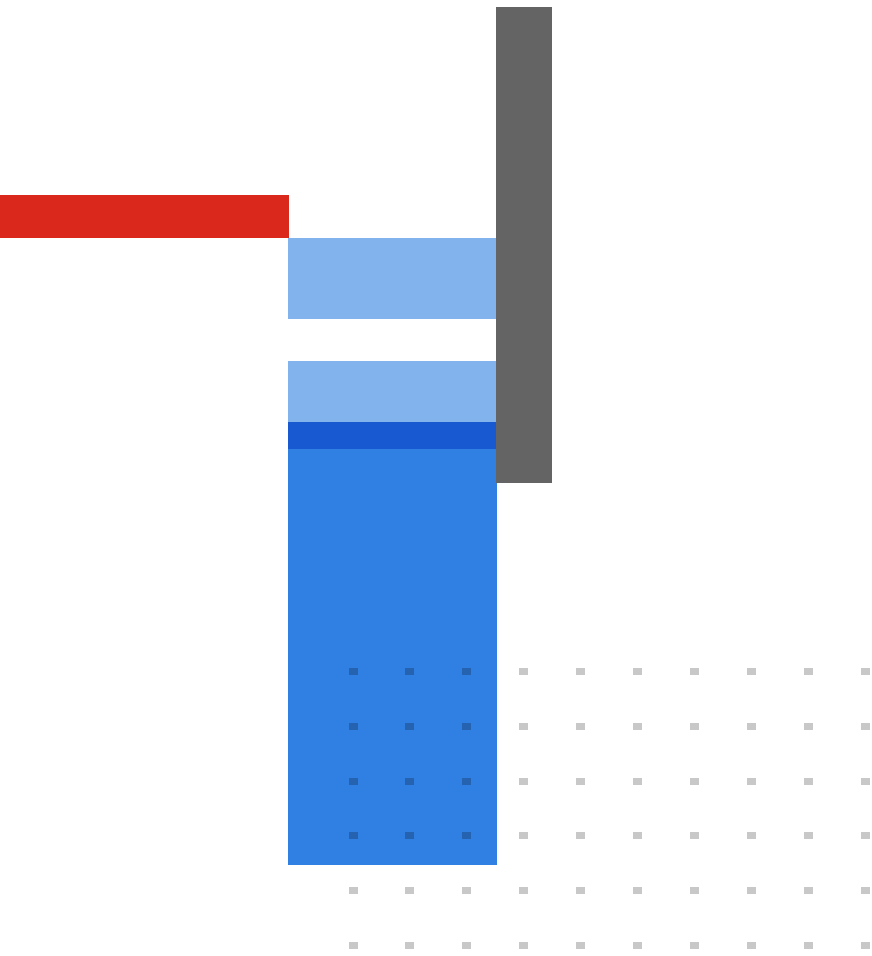
FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE's) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

Fortinet CSR 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

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

June 2, 2023

<https://www.uritprice.com>

FG-3500F-DAT-R10-20230602