

FortiGate 6000F Series

FG-6300F/-DC, FG-6301F/-DC, FG-6500F/-DC, and FG-6501F/-DC



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and WAN Edge Infrastructure.

Secure 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 6000F Series delivers high performance security-driven networks to large enterprises and service providers 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 6000F 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 6000F automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

Model	IPS	NGFW	Threat Protection	Interfaces
6300F/6301F	110 Gbps	90 Gbps	60 Gbps	Multiple 40/100 GE QSFP28, 1/10/25 GE SFP28, 1/10 GE SFP+ and GE RJ45 slots
6500F/6501F	170 Gbps	150 Gbps	100 Gbps	Multiple 40/100 GE QSFP28, 1/10/25 GE SFP28, 1/10 GE SFP+ and GE RJ45 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 NAC 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 6 NP6

Fortinet's new breakthrough SPU NP6 network processor works in line with FortiOS functions delivering:

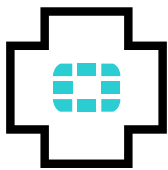
- Superior firewall performance for IPv4/IPv6, SCTP, and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing



Content Processor 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-any where models, SD-Branch, and cloud-first WAN use cases
 - Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing
-



Mobile Security for 4G, 5G, and IoT

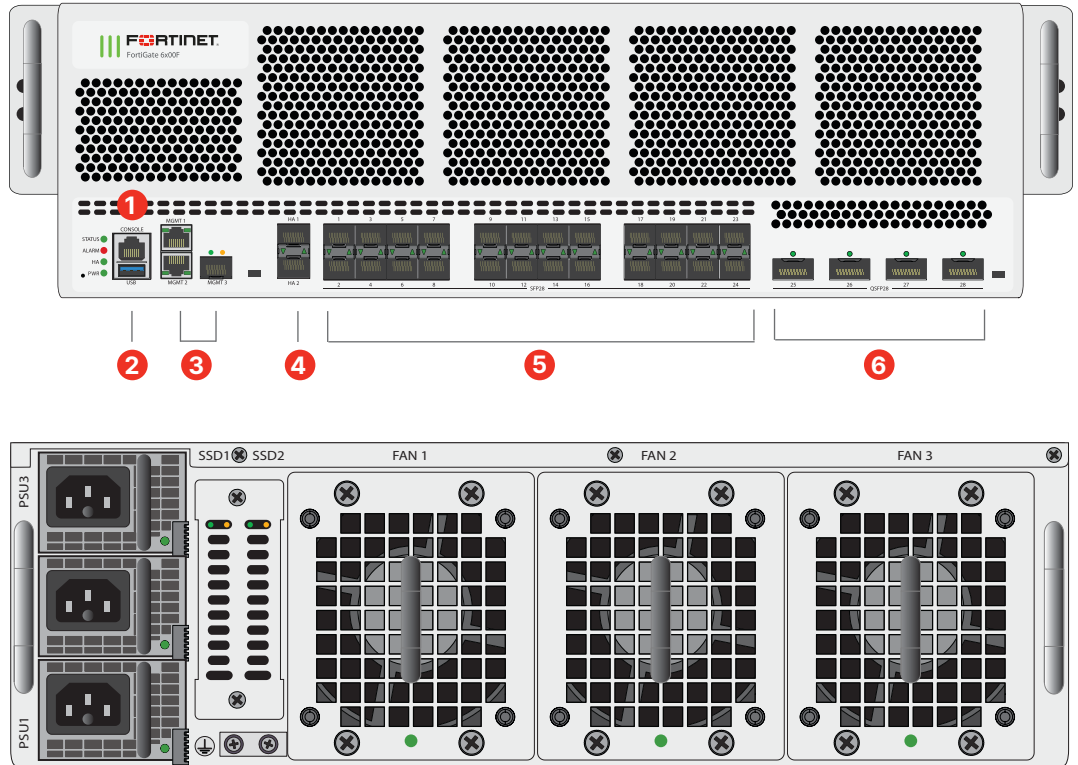
- SPU-accelerated, high performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/ DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- RAN Access Security with highly scalable and highest-performing IPsec aggregation and control Security Gateway (SecGW)
- User plane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

Datacenter Deployment (NGFW, IPS, Segmentation)



Hardware

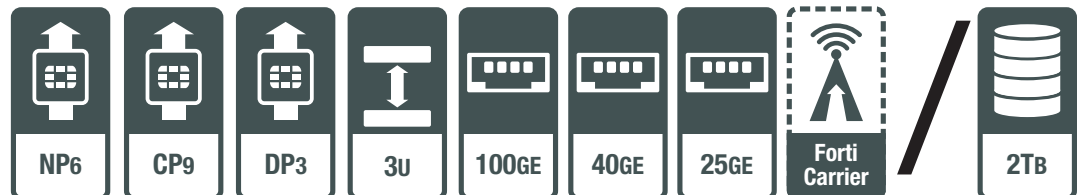
FortiGate FG-6300F/-DC, FG-6301F/-DC, FG-6500F/-DC, FG-6501F/-DC



Interfaces

1. Console Port
2. USB Port
3. 2 x GE RJ45, 1 X 1/10 GE SFP+ Management Ports
4. 2 x 10 GE SFP+ HA Slots
5. 24 x 1/10/25 GE SFP28 Slots
6. 4 x 40/100 GE QSFP28 Slots

Hardware Features



Specifications

FORTIGATE	6300F/-DC 6301F/-DC	6500F/-DC 6501F/-DC
Interfaces and Modules		
Hardware Accelerated 40/100 GE QSFP28 Slots		4
Hardware Accelerated 1/10/25 GE SFP28 Slots		24
Hardware Accelerated 10 GE SFP+ Slots		3
GE RJ45 Management Ports		2
USB Port		1
Console Port		1
Onboard Storage	2x 1 TB NVMe (for 6301F and 6501F only)	
Included Transceivers	2x SFP+ (SR 10 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	110 Gbps	170 Gbps
NGFW Throughput ^{2,4}	90 Gbps	150 Gbps
Threat Protection Throughput ^{2,5}	60 Gbps	100 Gbps
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	239 / 238 / 135 Gbps	239 / 238 / 135 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	239 / 238 / 135 Gbps	239 / 238 / 135 Gbps
Firewall Latency (64 byte, UDP)	4.80 µs	4.80 µs
Firewall Throughput (Packet per Second)	202.5 Mpps	202.5 Mpps
Concurrent Sessions (TCP)	120 Million	200 Million
New Sessions/Second (TCP)	2 Million	3 Million
Firewall Policies	200 000	200 000
IPsec VPN Throughput (512 byte) ¹	96 Gbps	160 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	16 000	16 000
Client-to-Gateway IPsec VPN Tunnels	90 000	90 000
SSL-VPN Throughput	9 Gbps	9 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30 000	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	66 Gbps	110 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³	30 000	50 000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	10 Million	18 Million
Application Control Throughput (HTTP 64K) ²	150 Gbps	220 Gbps
CAPWAP Throughput (HTTP 64K)	N/A	N/A
Virtual Domains (Default / Maximum)		10 / 500
Maximum Number of FortiSwitches Supported		256
Maximum Number of FortiAPs (Total / Tunnel)		N/A
Maximum Number of FortiTokens		20 000
High Availability Configurations	Active-Active (FGSP), 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.

FORTIGATE	6300F/-DC 6301F/-DC	6500F/-DC 6501F/-DC
Dimensions and Power		
Height x Width x Length (inches)	5.20 × 17.20 × 26.18	5.3 × 17.2 × 27.3
Height x Width x Length (mm)	132 × 437 × 665	133 × 437 × 694
Weight	67.68 lbs (30.7 kg) 69.00 lbs (31.3 kg)	78.26 lbs (35.5 kg) 79.59 lbs (36.1 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 3 RU	
AC Power Supply	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	977 W / 1,217 W 977 W / 1,237 W	1,308 W / 1,548 W 1,328 W / 1,568 W
AC Current (Maximum)	30A@100VAC, 20A@240VAC	
DC Power Supply	-48 to -60V DC	
DC Current (Maximum)	25–32A (x2)	
Heat Dissipation	4153 BTU/h / 4221 BTU/h	5282 BTU/h / 5350 BTU/h
Power Supply Efficiency Rating	80Plus Compliant	
Redundant Power Supplies	2+1 Redundant / 1+1 Redundant if using high line power Hot Swappable	
Fan Trays	Hot Swappable	
Operating Environment and Certifications		
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	-31°–158°F (-35°–70°C)	
Humidity	10%–90% non-condensing	
Noise Level	57.43 dBA	
Forced Airflow	Front to Back	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6/IPv6	

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.



Ordering Information

Product	SKU	Description
FortiGate 6300F	FG-6300F	4 × 40/100 GE QSFP28 slots, 24 × 1/10/25 GE SFP28 slots, 2 × 1 GE RJ45 management ports, 2 × 10 GE SFP+ HA ports, 1 × 1/10 GE SFP+ management port, and 3x AC power supplies.
FortiGate 6300F-DC	FG-6300F-DC	4 × 100GE QSFP28 slots, 24 × 25GE SFP28 slots, 3 × 10GE SFP+ slots, 2 x GE RJ45 MGMT port, and 2 x DC power supplies.
FortiGate 6301F	FG-6301F	4 × 40/100 GE QSFP28 slots, 24 × 1/10/25 GE SFP28 slots, 2 × 1 GE RJ45 management ports, 2 × 10 GE SFP+ HA ports, 1 × 1/10 GE SFP+ management port, 2 × 1 TB NVMe, and 3x AC power supplies.
FortiGate 6301F-DC	FG-6301F-DC	4 × 100/40GE QSFP28 slots, 24 × 25/10GE SFP+ slots, 2 × 1GE RJ45 management ports, 2 × 10GE SFP+ HA ports, 1 × 10GE SFP+ MGMT port, 2 × 1TB NVMe, and 2 x DC power supplies.
FortiGate 6500F	FG-6500F	4 × 40/100 GE QSFP28 slots, 24 × 1/10/25 GE SFP28 slots, 2 × 1 GE RJ45 management ports, 2 × 10 GE SFP+ HA ports, 1 × 1/10 GE SFP+ management port, and 3x AC power supplies.
FortiGate 6500F-DC	FG-6500F-DC	4 × 100/40GE QSFP28 slots, 24 × 25/10GE SFP+ slots, 2 × 1GE RJ45 management ports, 2 × 10GE SFP+ HA ports, 1 × 10GE SFP+ MGMT port and 2 x DC power supplies.
FortiGate 6501F	FG-6501F	4 × 40/100 GE QSFP28 slots, 24 × 1/10/25 GE SFP28 slots, 2 × 1 GE RJ45 management ports, 2 × 10 GE SFP+ HA ports, 1 × 1/10 GE SFP+ management port, 2 × 1 TB NVMe, and 3x AC power supplies.
FortiGate 6501F-DC	FG-6501F-DC	4 × 100/40GE QSFP28 slots, 24 × 25/10GE SFP+ slots, 2 × 1GE RJ45 management ports, 2 × 10GE SFP+ HA ports, 1 × 10GE SFP+ MGMT port, 2 × 1TB NVMe, and 2 x DC power supplies.
Training		
FortiGate Chassis-based Firewall Platform (FGT 6000 series) Training - 2 days	FT-FGT-CHS-6K	<p>Course description: https://training.fortinet.com/local/staticpage/view.php?page=library_fortigate-6000-series</p> <p>Upcoming sessions: https://training.fortinet.com/calendar/view.php/Course:FortiGate_6000_Series</p> <p>Price includes lab access and course material (Lab and Study guides). Exam voucher not included.</p>
Optional Accessories/Spares		
Optional Accessories/Spares	SKU	Description
1GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1GE SFP SX Transceiver Module	FN-TRAN-SX	1GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1GE SFP LX Transceiver Module	FN-TRAN-LX	1GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10GE Copper SFP+ RJ45 Transceiver (30m range)	FN-TRAN-SFP+GC	10GE copper SFP+ RJ45 Fortinet Transceiver (30m range) for systems with SFP+ slots.
10GE SFP+ Transceiver Module, short range	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10GE SFP+ Transceiver Module, long range	FN-TRAN-SFP+LR	10GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10Gbase-ER SFP+ Transceivers	FN-TRAN-SFP+ER	10Gbase-ER SFP+ transceivers for FortiSwitch and FortiGate, 1550nm. Single Mode. 40km range for systems with SFP+ Slots.
25GE SFP28 Transceiver Module, short range	FN-TRAN-SFP28-SR	25GE/10GE Dual Rate SFP28 transceiver module, short range for all systems with SFP28/SFP+ slots.
25GE SFP28 Transceiver Module, long range	FN-TRAN-SFP28-LR	25GE SFP28 transceiver module, long range for all systems with SFP28 slots.
40GE QSFP+ Transceiver Module, short range	FN-TRAN-QSFP+SR	40GE QSFP+ transceivers, short range for all systems with QSFP+ Slots.
40GE QSFP+ Transceiver Module, long range	FN-TRAN-QSFP+LR	40GE QSFP+ transceivers, long range for all systems with QSFP+ Slots.
100GE QSFP28 Transceiver Module	FN-TRAN-QSFP28-SR	100GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 Slots.
100 GE QSFP28 Transceiver Module, 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 Transceiver Module	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 Slots.
Fan Tray	SP-FG4K6K-FAN	Spare Hotswappable Fan Module for FG-420xF/440xF/6000F.
AC 1500W Power Supply	FG-7040E-PS-AC	1500W AC Power Supply for FG-7030E,FG-7040E, 6000F and FG-3900E series (not compatible for use with FG-7060E) , does not include SP-FGPCORC15-XX power cord.
AC 2000W Power Supply	SP-FG4000F-PS	2000W AC power supply for 4000F and 6000F series, does not include SP-FGPCORC15-XX power cord.
DC Power Supply	SP-FG4000F-DC-PS	DC power supply for FG-4200F-DC/4201F-DC, FG-4400F-DC/4401F-DC and FG-6000F-DC.
Power Cord	SP-FGPCORC15-XX	6 ft power cord, 15A125V XXX, PSE BLACK ROHS-6, for FG-3900E, 4000F, 6000F and 7000E/F Series.



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				included with FortiCare Subscription
	GeolP DB Updates				included with FortiCare Subscription
	Device/OS Detection Signatures				included with FortiCare Subscription
	Trusted Certificate DB Updates				included with FortiCare Subscription
	DDNS (v4/v6) Service				included with FortiCare Subscription

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 © 2022 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.

November 15, 2022

FG-6000F-DAT-R29-20221115