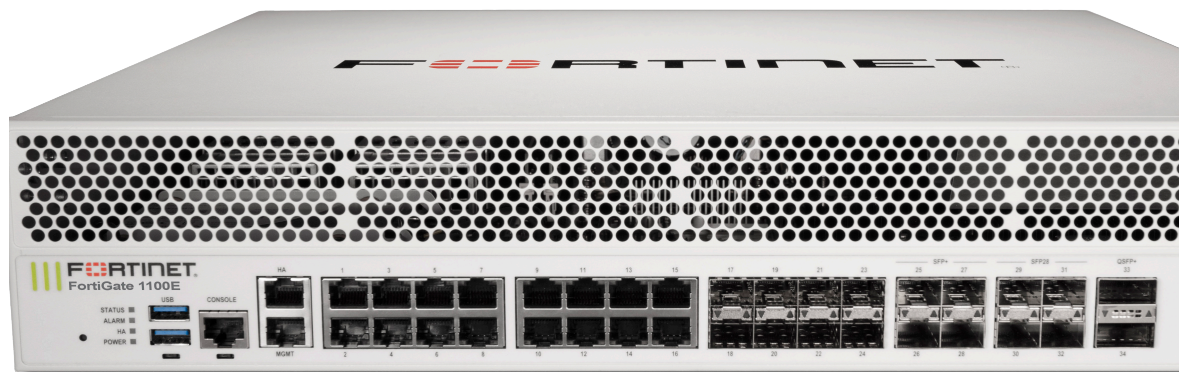


# FortiGate 1100E Series

FG-1100E/-DC and FG-1101E



## 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 1100E 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 1100E 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 1100E automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

IPS	NGFW	Threat Protection	Interfaces
12.5 Gbps	9.8 Gbps	7.1 Gbps	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP, and 40 GE QSFP+ slots



Available in



Appliance



Virtual



Hosted



Cloud



Container

## FortiOS Everywhere

### FortiOS, Fortinet's Advanced Operating System

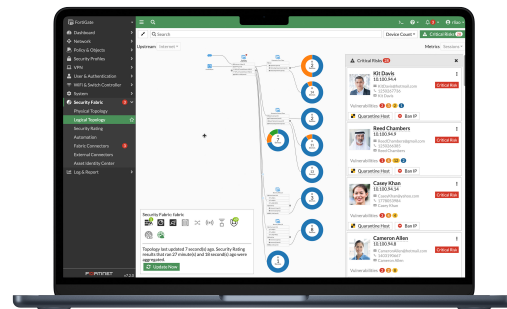
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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

### Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

---

### Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

---

### SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

---

### Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

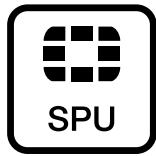
---

### OT Security

The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.



## 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



*Intuitive view and clear insights into network security posture with FortiManager*

### Centralized Network and Security Management at Scale

FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving as the fundamental component for deploying Hybrid Mesh Firewalls.

## Use Cases



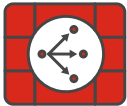
### Next Generation Firewall (NGFW)

- 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

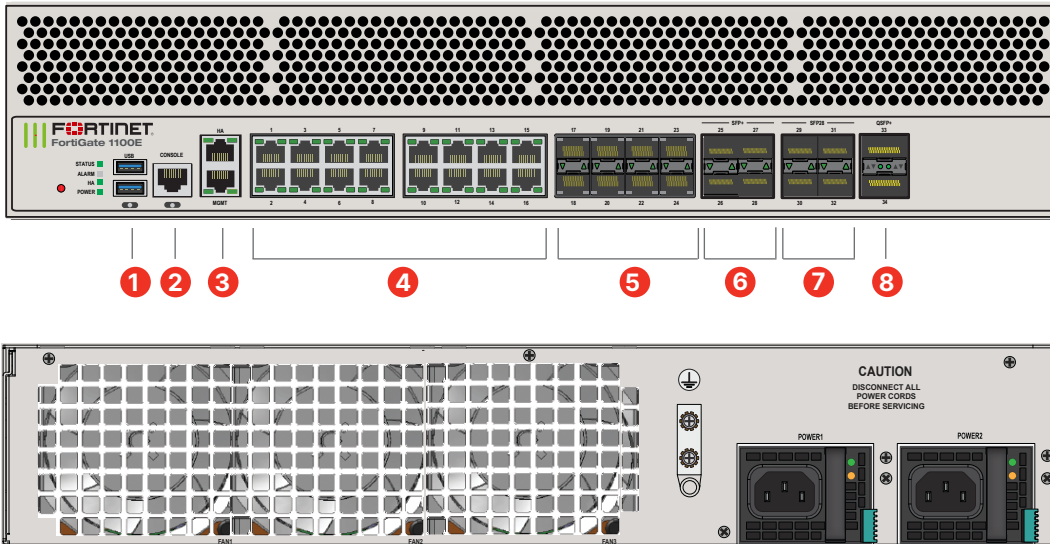
- SPU-accelerated, high performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/ DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- RAN Access Security with highly scalable and highest-performing IPsec aggregation and control Security Gateway (SecGW)
- User plane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

### Datacenter Deployment (NGFW, IPS, Segmentation)



## Hardware

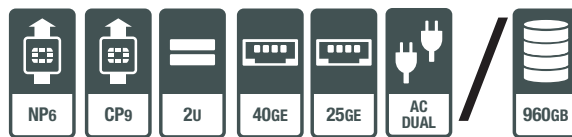
### FortiGate 1100E Series



### Interfaces

1. 2 x USB Ports
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/HA Ports
4. 16 x GE RJ45 Ports
5. 8 x GE SFP Slots
6. 4 x 10 GE SFP+ Slots / GE SFP Slots
7. 4 x 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
8. 2 x 40 GE QSFP+ Slots

### Hardware Features



### High-Speed Connectivity

High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 1100E series provides high speed interfaces, simplifying network designs without relying on additional devices to bridge desired connectivity.

## Specifications

	FG-1100E/-DC	FG-1101E
<b>Interfaces and Modules</b>		
Hardware Accelerated 40 GE QSFP+ Slots		2
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		4
Hardware Accelerated 10 GE SFP+ Slots / GE SFP Slots		4
Hardware Accelerated GE SFP Slots		8
Hardware Accelerated GE RJ45 Ports		16
GE RJ45 Management / HA Ports		2
USB Ports (Client / Server)		1 / 2
Console Port		1
Onboard Storage	0	2x 480 GB SSD
Included Transceivers	2x SFP (SX 1 GE)	
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		12.5 Gbps
NGFW Throughput <sup>2,4</sup>		9.8 Gbps
Threat Protection Throughput <sup>2,5</sup>		7.11 Gbps
<b>System Performance and Capacity</b>		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		80 / 80 / 45 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		80 / 80 / 45 Gbps
Firewall Latency (64 byte, UDP)		2.76 µs
Firewall Throughput (Packet per Second)		67.5 Mpps
Concurrent Sessions (TCP)		8 Million
New Sessions/Second (TCP)		500 000
Firewall Policies		100 000
IPsec VPN Throughput (512 byte) <sup>1</sup>		48 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		20 000
Client-to-Gateway IPsec VPN Tunnels		100 000
SSL-VPN Throughput		8.4 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		10 000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		10 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		6500
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		780 000
Application Control Throughput (HTTP 64K) <sup>2</sup>		26 Gbps
CAPWAP Throughput (HTTP 64K)		43 Gbps
Virtual Domains (Default / Maximum)		10 / 250
Maximum Number of FortiSwitches Supported		196
Maximum Number of FortiAPs (Total / Tunnel)		4096 / 2048
Maximum Number of FortiTokens		20 000
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-1100E/-DC	FG-1101E
<b>Dimensions and Power</b>		
Height x Width x Length (inches)	3.5 × 17.44 × 17.62	
Height x Width x Length (mm)	88.9 × 443 × 447.4	
Weight	24.9 lbs (11.3kg)	25.4 lbs (11.55 kg)
Form Factor (supports EIA/ non-EIA standards)	Rack Mount, 2 RU	
AC Power Input	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	217 W / 336 W	222 W / 346 W
AC Current (Maximum)	6A@120V, 3A@240V	
Heat Dissipation	1147 BTU/h	1181 BTU/h
DC Power Input (FG-1100E-DC)	-48V DC	--
DC Current (Maximum)	11.5A	--
Redundant Power Supplies (Hot Swappable)	Yes (Default dual AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
<b>Operating Environment and Certifications</b>		
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	10% to 90% non-condensing	
Noise Level	66.7 dBA	
Forced Airflow	Front to Back	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	USGv6/IPv6	

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

<sup>1</sup> IPsec VPN performance test uses AES256-SHA256.

<sup>2</sup> IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

<sup>3</sup> SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

<sup>4</sup> NGFW performance is measured with Firewall, IPS and Application Control enabled.

<sup>5</sup> Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.





## Ordering Information

Product	SKU	Description
FortiGate 1100E	FG-1100E	2× 40 GE QSFP+ slots, 4× 25 GE SFP28 slots, 4× 10 GE SFP+ slots, 8x GE SFP slots, 18x GE RJ45 ports (including 16x ports, 2x management/HA ports) SPU NP6 and CP9 hardware accelerated, and 2 AC power supplies.
FortiGate 1101E	FG-1101E	2× 40 GE QSFP+ slots, 4× 25 GE SFP28 slots, 4× 10 GE SFP+ slots, 8x GE SFP slots, 18x GE RJ45 ports (including 16x ports, 2x management/HA ports) SPU NP6 and CP9 hardware accelerated, 960 GB SSD onboard storage, and 2 AC power supplies.
FortiGate 1100E-DC	FG-1100E-DC	2× 40 GE QSFP+ slots, 4× 25 GE SFP28 slots, 4× 10 GE SFP+ slots, 8x GE SFP slots, 18x GE RJ45 ports (including 16x ports, 2x management/HA ports) SPU NP6 and CP9 hardware accelerated, and 2 DC power supplies.
Optional Accessories	SKU	Description
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1100/1101E, FG-1200D, FG-1500D/-DC, FG-2000E, FG-2500E, 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	SP-FG300E-PS	AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FG-1100/1101E, FAZ-200F/FAZ-300F/FMG-200F and FAZ-800F/FMG-300F.
DC Power Supply	SP-FG300E-DC-PS	DC power supply for FG-1100E-DC
Transceivers	SKU	Description
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+ Transceiver Module, 80km Extreme Long Range	FN-TRAN-SFP+ZR	10 GE SFP+ transceiver module, 80km extreme long range, 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+ Transceivers, Short Range, BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceivers, short range BiDi for 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.
Cables	SKU	Description
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.
40 GE QSFP+ to 4× 10 GE SFP+ Optical Breakout	FG-TRAN-QSFP+4XSFP	40 GE QSFP+ Parallel Breakout Active Optical Cable with 1m length for all systems with QSFP+ slots.
40 GE QSFP+ to 4xSFP+ Optical breakout 5m	FG-TRAN-QSFP+4SFP-5	40 GE QSFP+ Parallel Breakout MPO to 4xLC connectors, 5m reach, transceivers not included.



## Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			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, AI-based Heuristic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention	•	•		
	Data Loss Prevention (DLP) <sup>1</sup>	•	•		
	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 <sup>1</sup>	•			
	Application Control			included with FortiCare Subscription	
	Inline CASB		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	•			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth) <sup>2</sup>	•			
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 <sup>2</sup>	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Device/OS Detection, GeolIPs, 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.

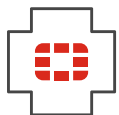
2. Desktop Models only.

3. Not available for FG/FWF/FGR 30 to 60, 80E, 90E series from 7.4.4 onwards.



### 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 Services

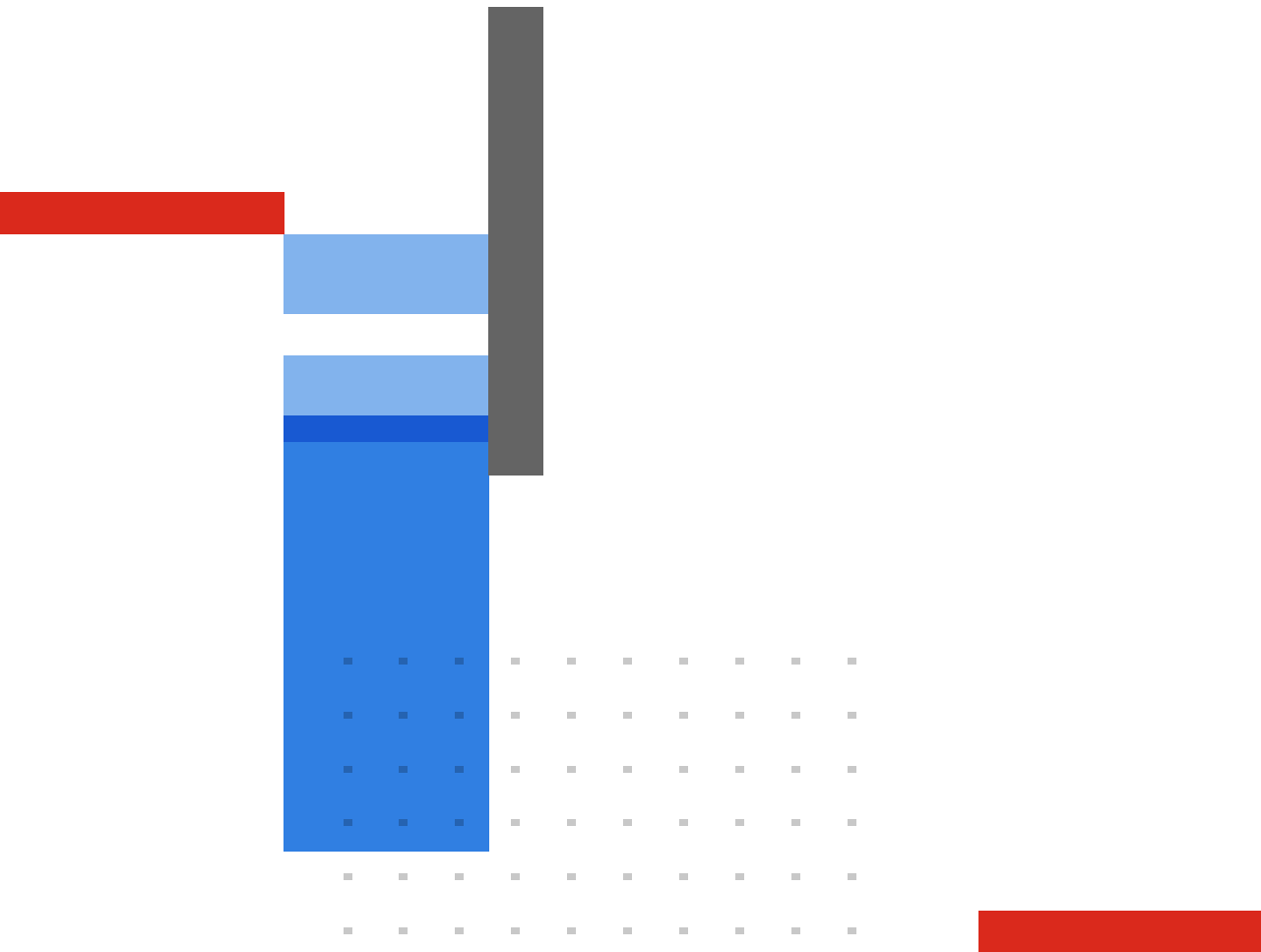
Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an Extended End-of-Engineering-Support of 18 months, providing flexibility. Access the intuitive FortiCare Elite Portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.



---

## 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](http://www.fortinet.com)

Copyright © 2024 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 Chief Legal Officer, 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.