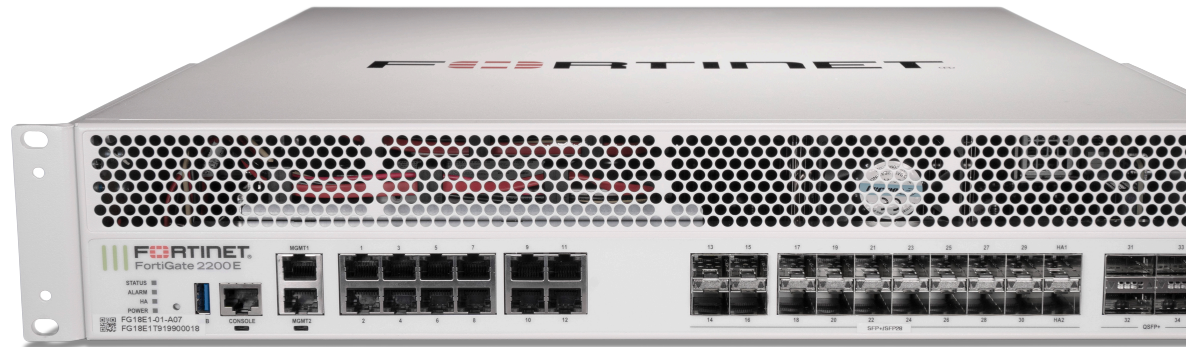


FortiGate 2200E Series

FG-2200E and FG-2201E



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.

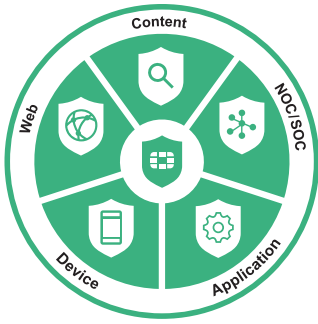
High performance with flexibility

The FortiGate 2200E 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 2200E 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 2200E automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

IPS	NGFW	Threat Protection	Interfaces
21.8 Gbps	13.5 Gbps	11 Gbps	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP, and 40 GE QSFP+ slots



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

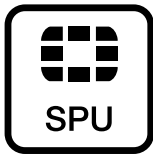
Includes tier-one hunting and automation, log location, 24x7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

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:

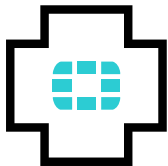
- Superior firewall performance for IPv4/IPv6, SCTP, and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing



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:

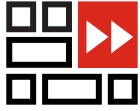
- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload, and accelerated antivirus processing



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



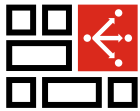
Next Generation Firewall (NGFW)

- 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

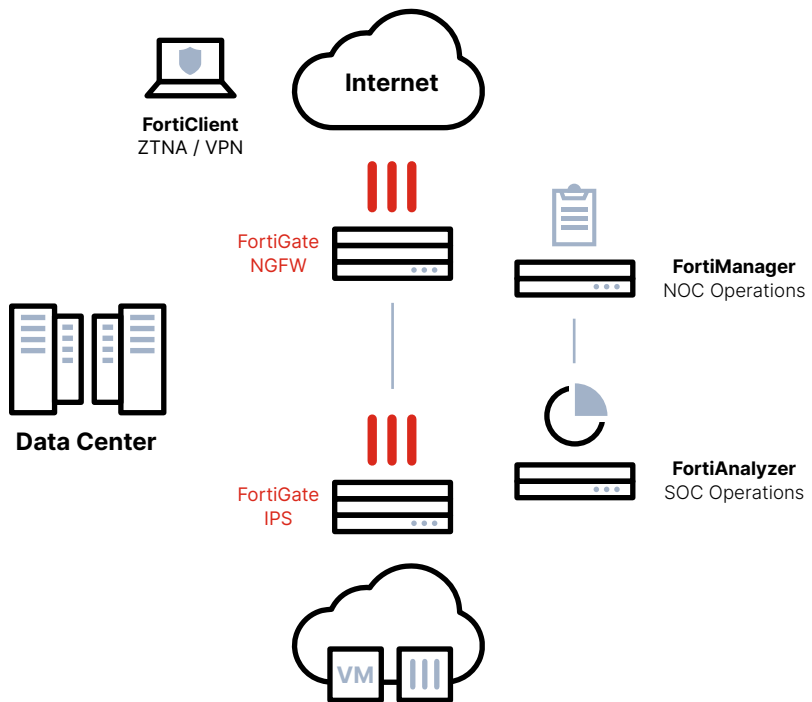
- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
 - Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
 - Achieve operational efficiencies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



Mobile Security for 4G, 5G, and IoT

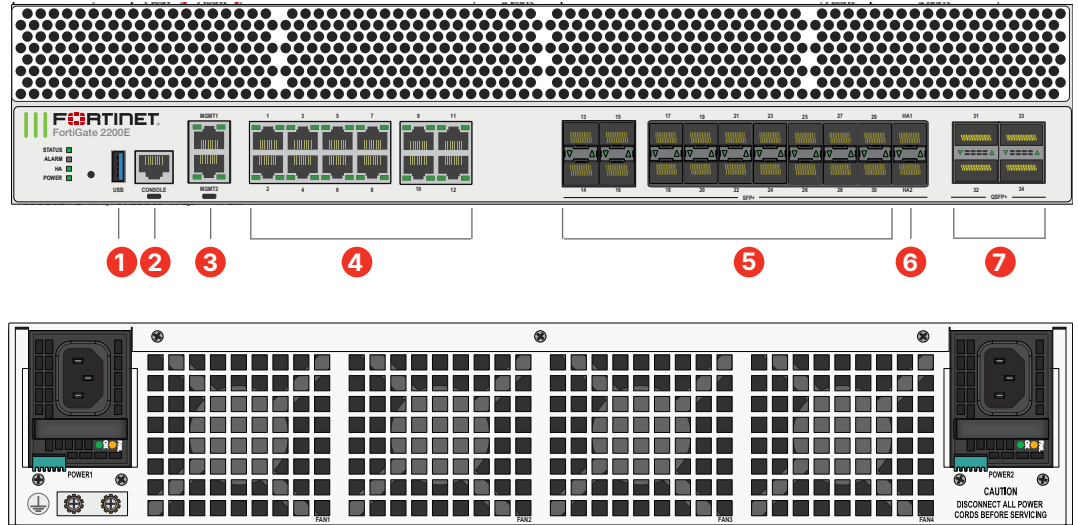
- SPU-accelerated, high performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/ DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- RAN Access Security with highly scalable and highest-performing IPsec aggregation and control Security Gateway (SecGW)
- User plane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

Datacenter Deployment (NGFW, IPS, Segmentation)



Hardware

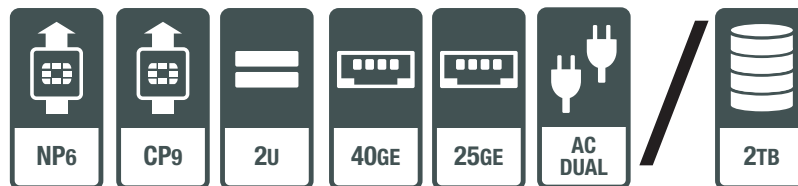
FortiGate 2200E Series



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 Management Ports
4. 12 x GE RJ45 Ports
5. 18 × 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
6. 2 × 25 GE SFP28 / 10 GE SFP+ / GE SFP HA Slots
7. 4 × 40 GE QSFP+ Slots

Hardware Features



Specifications

	FORTIGATE 2200E	FORTIGATE 2201E
Interfaces and Modules		
Hardware Accelerated 40 GE QSFP+ Slots		4
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP HA Slots		2
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		18
Hardware Accelerated GE RJ45 Ports		12
GE RJ45 Management Ports		2
USB Port		1
Console Port		1
Onboard Storage	0	2x 1 TB SSD
Included Transceivers	2x SFP+ (SR 10 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	21.8 Gbps	
NGFW Throughput ^{2,4}	13.5 Gbps	
Threat Protection Throughput ^{2,5}	11 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	158 / 155 / 100 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	158 / 155 / 100 Gbps	
Firewall Latency (64 byte, UDP)	3.09 µs	
Firewall Throughput (Packet per Second)	150 Mpps	
Concurrent Sessions (TCP)	24 Million	
New Sessions/Second (TCP)	500 000	
Firewall Policies	100 000	
IPsec VPN Throughput (512 byte) ¹	98 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	20 000	
Client-to-Gateway IPsec VPN Tunnels	100 000	
SSL-VPN Throughput	10 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30 000	
SSL Inspection Throughput (IPS, avg. HTTPS) ³	17 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) ³	9500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	2.5 Million	
Application Control Throughput (HTTP 64K) ²	52 Gbps	
CAPWAP Throughput (HTTP 64K)	60 Gbps	
Virtual Domains (Default / Maximum)	10 / 500	
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	

	FORTIGATE 2200E	FORTIGATE 2201E
Dimensions and Power		
Height x Width x Length (inches)	3.5 × 17.44 × 21.89	
Height x Width x Length (mm)	88.9 × 443 × 556	
Weight	40.0 lbs (18.2 kg)	41.4 lbs (18.8 kg)
Form Factor	Rack Mount, 2 RU	
AC Power Supply	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	408 W / 571 W	412 W / 577 W
Current (Maximum)	12A@100V, 9A@240V	
Heat Dissipation	1948 BTU/h	1968 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	10%–90% non-condensing	
Noise Level	70 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	

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.



Ordering Information

Product	SKU	Description
FortiGate 2200E	FG-2200E	4× 40 GE QSFP+ slots, 20× 25 GE SFP28 slots (including 18x ports, 2x HA ports), 14x GE RJ45 ports (including 12x ports, 2x management ports), SPU NP6 and CP9 hardware accelerated, and dual AC power supplies.
FortiGate 2201E	FG-2201E	4× 40 GE QSFP+ slots, 20× 25 GE SFP28 slots (including 18x ports, 2x HA ports), 14x GE RJ45 ports (including 12x ports, 2x management ports), SPU NP6 and CP9 hardware accelerated, and dual AC power supplies, with 2× 1 TB SSD onboard storage.
Optional Accessories	SKU	Description
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+ 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.
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+ Passive Direct Attach Cable	SP-CABLE-FS-QSFP+(1/3/5)	40GE QSFP+ Passive Direct Attach Cable, (1/3/5 m) for Systems with QSFP+ slots.
QSFP+ to 4xSFP+ Optical breakout 5m	FG-TRAN-QSFP+4SFP-5	40 G QSFP+ Parallel Breakout MPO to 4xLC connectors, 5m reach, transceivers not included.
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-2200E/2201E, FG-2500E, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3300E/3301E, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC.
AC Power Supply	SP-FG3800D-PS	AC power supply for FG-2200/2201E, FG-3300/3301E, FG-3400/3401E, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D.



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.

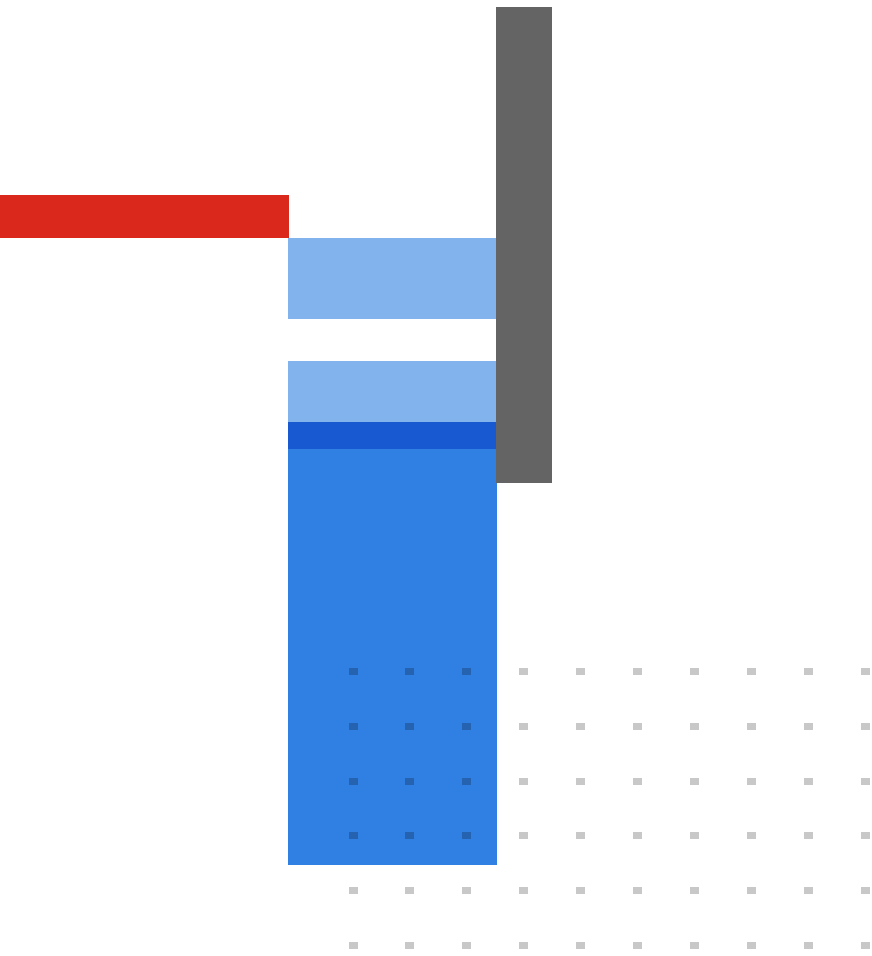
FortiCare Elite

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-2200E-DAT-R18-20221115