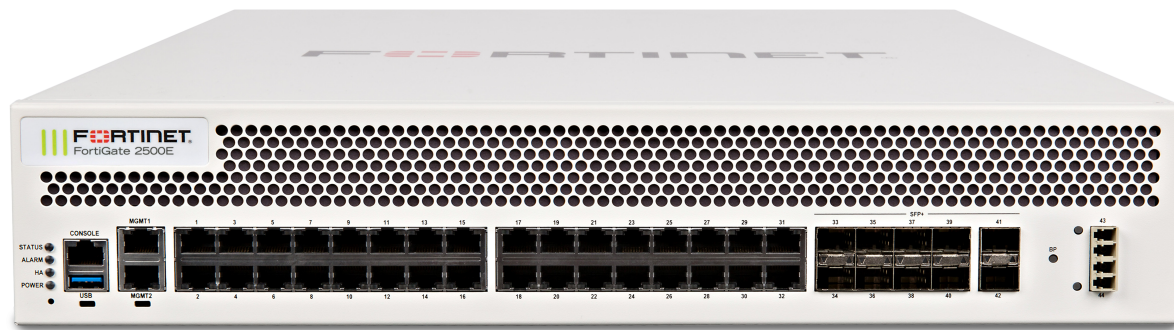**FORTINET**

FortiGate 2500E

FG-2500E

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 2500E 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 2500E 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 2500E Series automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

IPS	NGFW	Threat Protection	Interfaces
11.5 Gbps	9 Gbps	5.4 Gbps	Multiple GE RJ45, 10 GE SFP+ slots and Bypass 10 GE SFP+ ports

OS

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
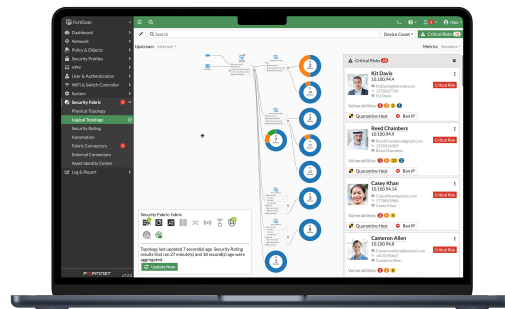
Intuitive easy to use view into the network and endpoint vulnerabilities
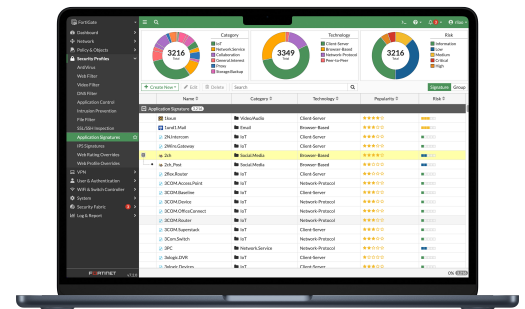
Visibility with FOS Application Signatures

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 inline 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
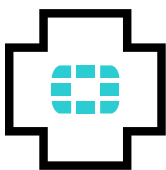
FortiCare Services

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
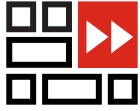
Next Generation Firewall (NGFW)

- 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
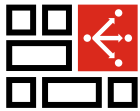
Secure SD-WAN

- 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

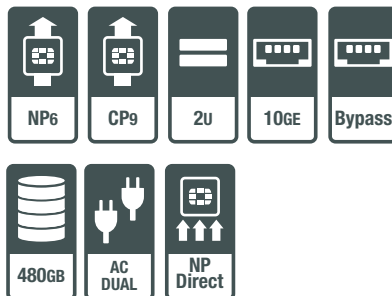**Datacenter Deployment** (NGFW, IPS, Segmentation)
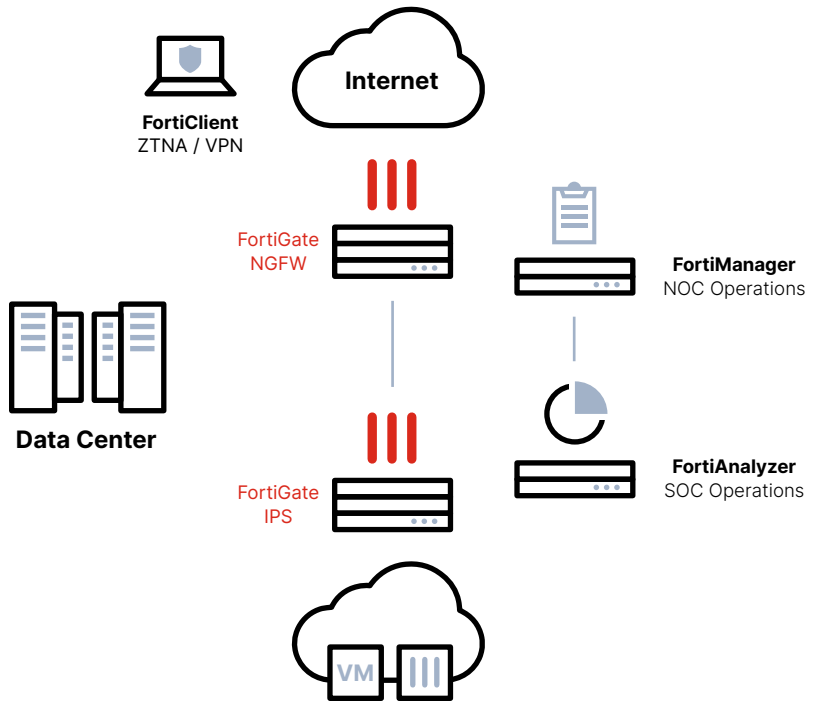
Hardware

FortiGate 2500E Series
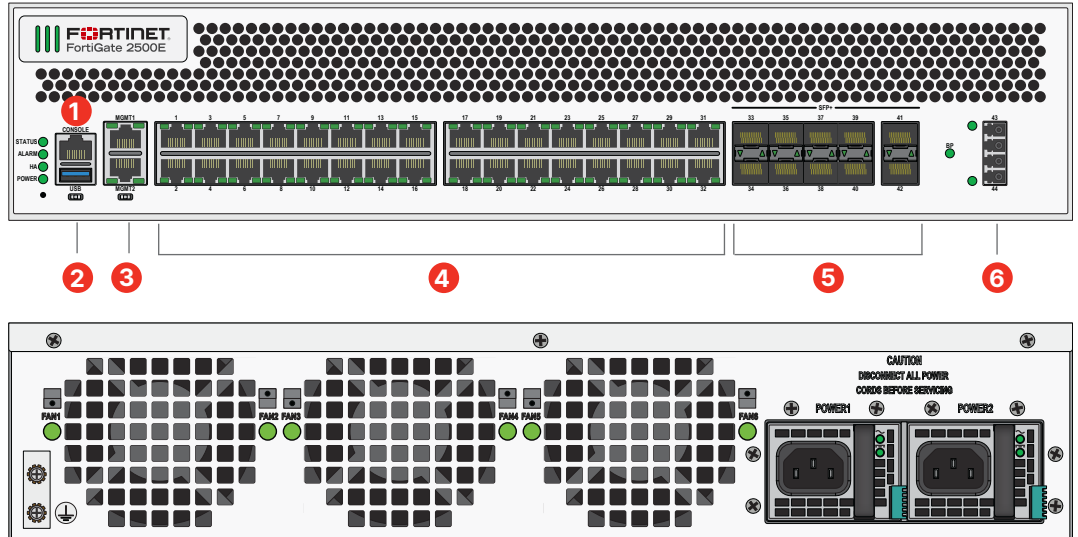
Interfaces

1. 1 x Console Port
2. 1 x USB Port
3. 2 x GE RJ45 Management Ports
4. 32 x GE RJ45 Ports
5. 10 × 10 GE SFP+ Slots
6. 2 × 10 GE SFP+ SR (LC Connector, bypass)

Hardware Features

Specifications

FORTIGATE 2500E	
Interfaces and Modules	
Hardware Accelerated 10 GE SFP+ Slots	10 + 2 bypass
Hardware Accelerated GE RJ45 Ports	32
GE RJ45 Management / HA Ports	2
USB Ports	1
Console Port	1
Internal Storage	1× 480 GB SSD
Included Transceivers	2x SFP+ (SR 10GE)
System Performance — Enterprise Traffic Mix	
IPS Throughput [2]	11.5 Gbps
NGFW Throughput [2, 4]	9 Gbps
Threat Protection Throughput [2, 5]	5.4 Gbps
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	150 / 150 / 95 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	150 / 150 / 95 Gbps
Firewall Latency (64 byte, UDP)	2.00 µs
Firewall Throughput (Packet per Second)	145.5 Mpps
Concurrent Sessions (TCP)	20 Million
New Sessions/Second (TCP)	500 000
Firewall Policies	100 000
IPsec VPN Throughput (512 byte) [1]	95 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	20 000
Client-to-Gateway IPsec VPN Tunnels	100 000
SSL-VPN Throughput	6 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	9.4 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	5500
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	2 Million
Application Control Throughput (HTTP 64K) [2]	20 Gbps
CAPWAP Throughput (1444 byte, UDP)	21 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 2500E	
Dimensions and Power	
Height x Width x Length (inches)	3.5 × 17.4 × 21.9
Height x Width x Length (mm)	88 × 442 × 555
Weight	38.5 lbs (17.6 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2 RU
Power	
Power Input	100–240V AC, 50/60 Hz
Maximum Current	9A
Power Consumption (Average / Maximum)	312 W / 470 W
Heat Dissipation	1604 BTU/h
Redundant Power Supplies	Yes, 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	58 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	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 2500E	FG-2500E	10× 10 GE SFP+ slots, 2× 10 GE bypass SFP+ (LC Adapter), 34x GE RJ45 ports (including 32x ports, 2x management/HA ports), SPU NP6 and CP9 hardware accelerated, 480 GB SSD onboard storage.
Optional Accessories		
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.
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, 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-3700D/-DC, FG-3700DX, FG-3810D/-DC, FG-3815D/-DC and FG-3950B/-DC.
AC Power Supply	SP-FG2000E-PS	AC power supply for FG-2000E and FG-2500E.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	**IPS Service**	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control	included with FortiCare Subscription			
	CASB SaaS Control	included with FortiCare Subscription			
SD-WAN and SASE Services	**SD-WAN Underlay Bandwidth and Quality Monitoring Service**	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	**FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates)** [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	**FortiCare Essentials**	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	**Internet Service (SaaS) DB Updates**	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Full features available when running FortiOS 7.4.1
2. Desktop Models only

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.
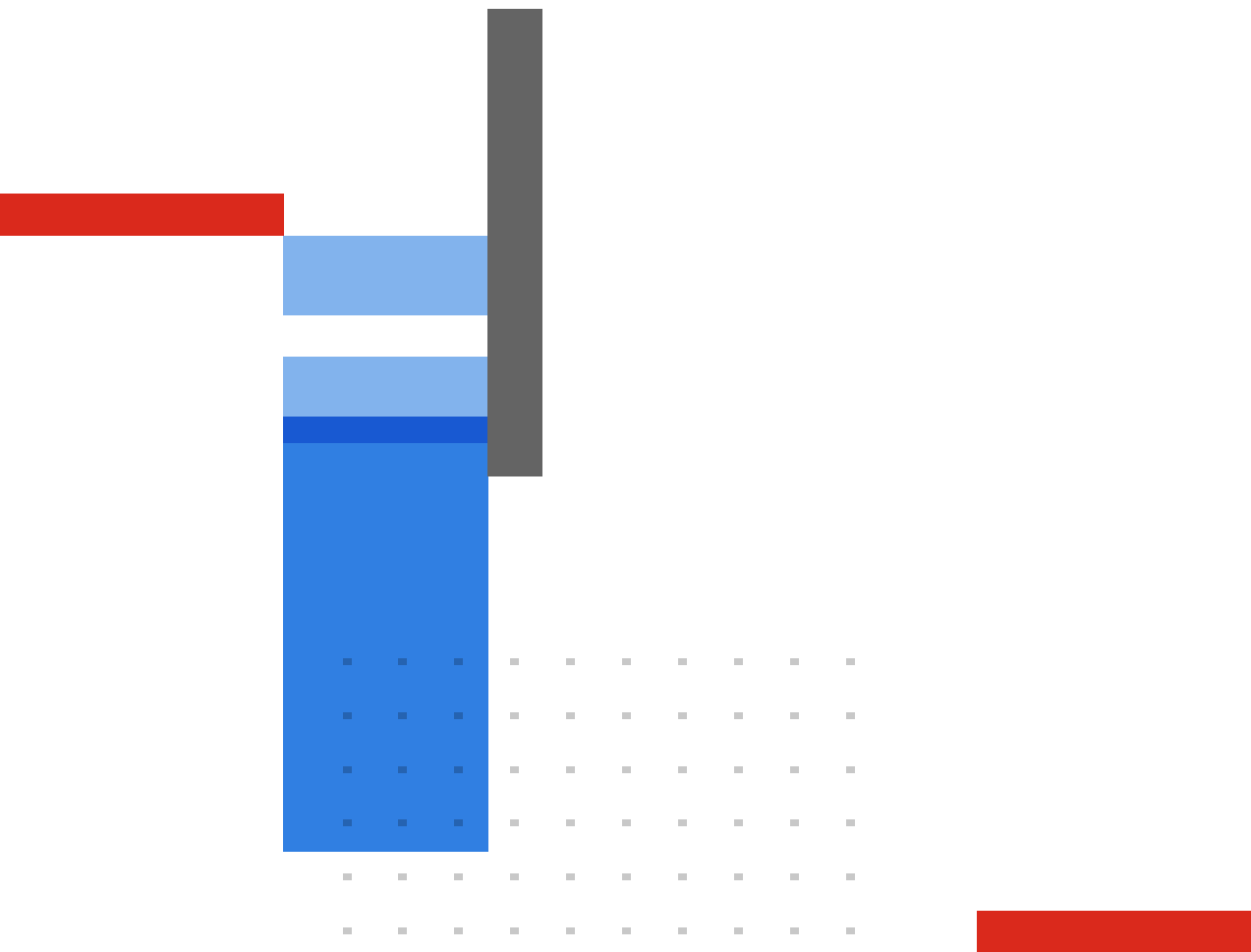
FortiCare Elite

FortiCare Elite offers enhanced SLAs and quick issue resolution through a dedicated support team. It provides single-touch ticket handling, extended Extended End-of-Engineering-Support for 18 months, and access to the new FortiCare Elite Portal for a 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.

F\u{2207}RTINET.

www.fortinet.com

October 20, 2023

FG-2500E-DAT-R25-20231020