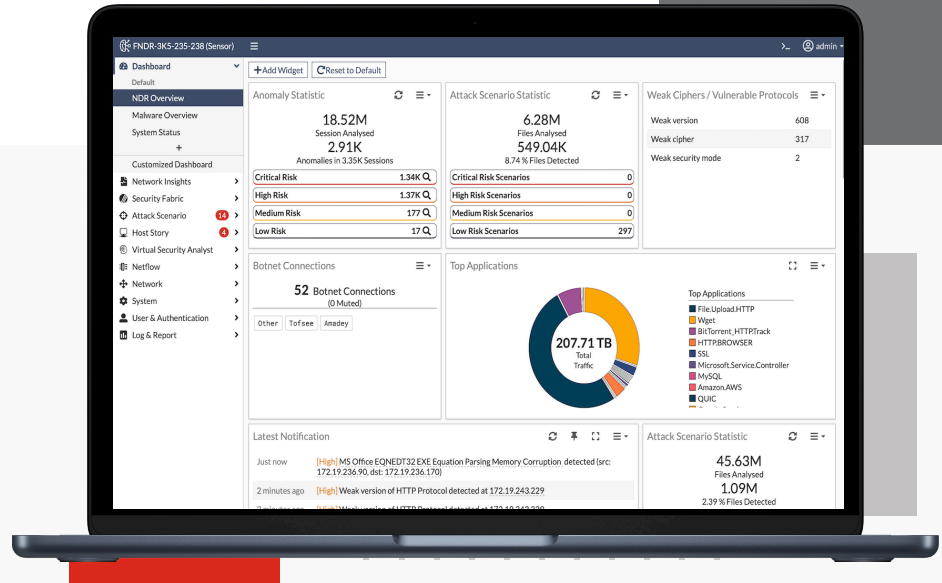


FortiNDR™ On Premise Solution



Highlights

- On premises deployment where no customer data leaves the network
- Ideally for government, air-gapped, military, and operational technology (OT) deployment
- High throughput Neural Networks for file-based scanning and malware classification
- Netflow ingestion support for security analytics
- AD integration support for device enrichment
- NDR Center and Sensor mode available for centralised management

Network Detection and Response

FortiNDR represents the future of artificial-intelligence (AI)-driven, network-based breach protection technology designed for short-staffed Security Operation Center (SOC) teams to identify, classify, and respond to threats, including those that are well-camouflaged. Supervised and unsupervised machine learning (ML) continuously analyze metadata, especially east-west data in datacentres, to identify threats, especially those which may be already persistent in the network.

FortiNDR significantly reduces the time to identify network anomalies and malicious content on your network and mitigate with Fortinet Security Fabric and third party integration.

Highlights

Available in



Appliance



VM



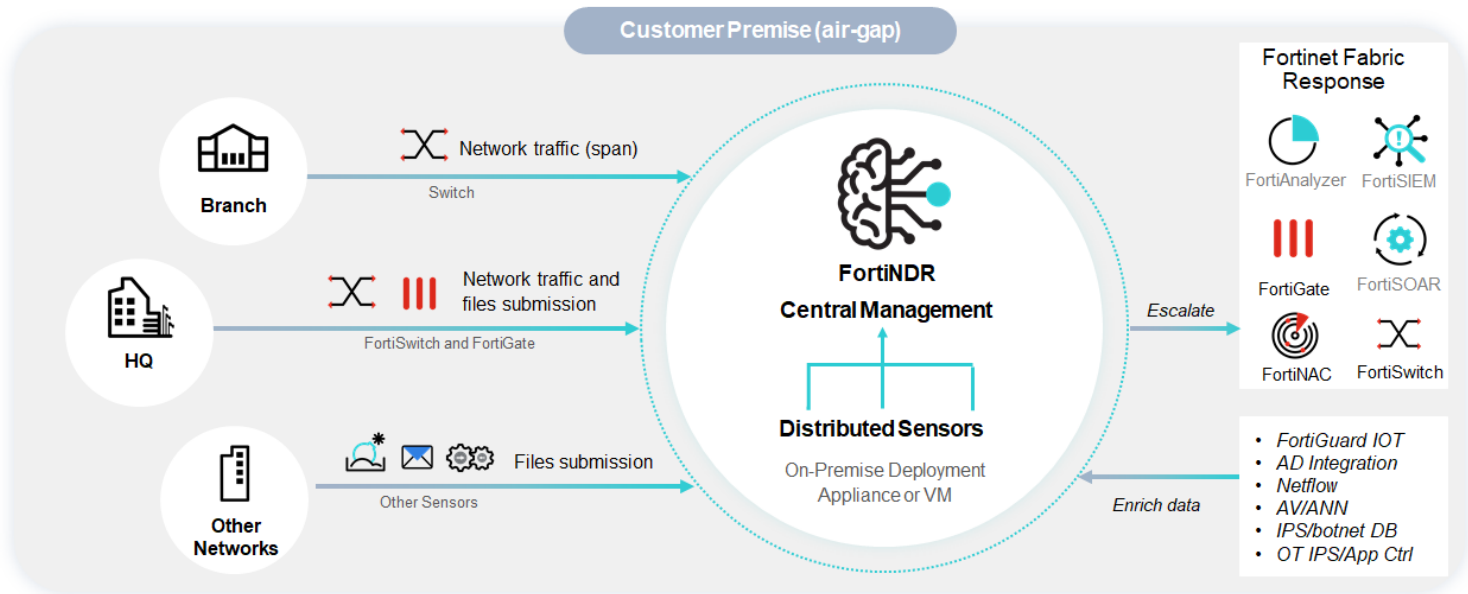
Public Cloud
(BYOL)

FortiNDR Key Features

- On Premise solution where no data leaves the customer network
- Integrate with Fortinet Security Fabric including FortiGate/FortiNAC/FortiSwitch quarantine, FortiAnalyzer/FortiSIEM log and report
- Supports standalone, center, and sensor modes for distributed deployment
- Patented high throughput malware scanning based on Artificial Neural Networks (ANN) ¹ to identify file-based attacks, with over 20+ malware attack scenarios
- Reduce malware detection and investigation time from minutes to seconds
- Detect North/South/East/West intrusions accurately
- Detect botnets and weakciphers on network
- Virtual Security Analyst™ to mimic experienced security analyst for outbreak, anomalies, and root causes for malware infections
- Provide on-premises learning to reduce false positives by analyzing organizational-specific traffic and adapting to newly disguised threats

¹ Patent # U.S. Serial No.: 16/053,479

FortiNDR On Premise SOC Deployment



Top Reasons for FortiNDR Solution

Shortage of Experienced SOC Analysts

Experience is the hardest thing to acquire in cybersecurity, especially in threat analysis, outbreak investigation, and malware research experience. FortiNDR provides Virtual Security Analyst™.

Breach Prevention

Using both ML and signature-based to identify breaches with high degree of confidence, including data enrichment on attacks.

AI-Powered Detection and Response for Cyber Attacks

Innovative threat actors disrupt cyber security through automated attacks designed to overwhelm or sneak past your SOC defenses.

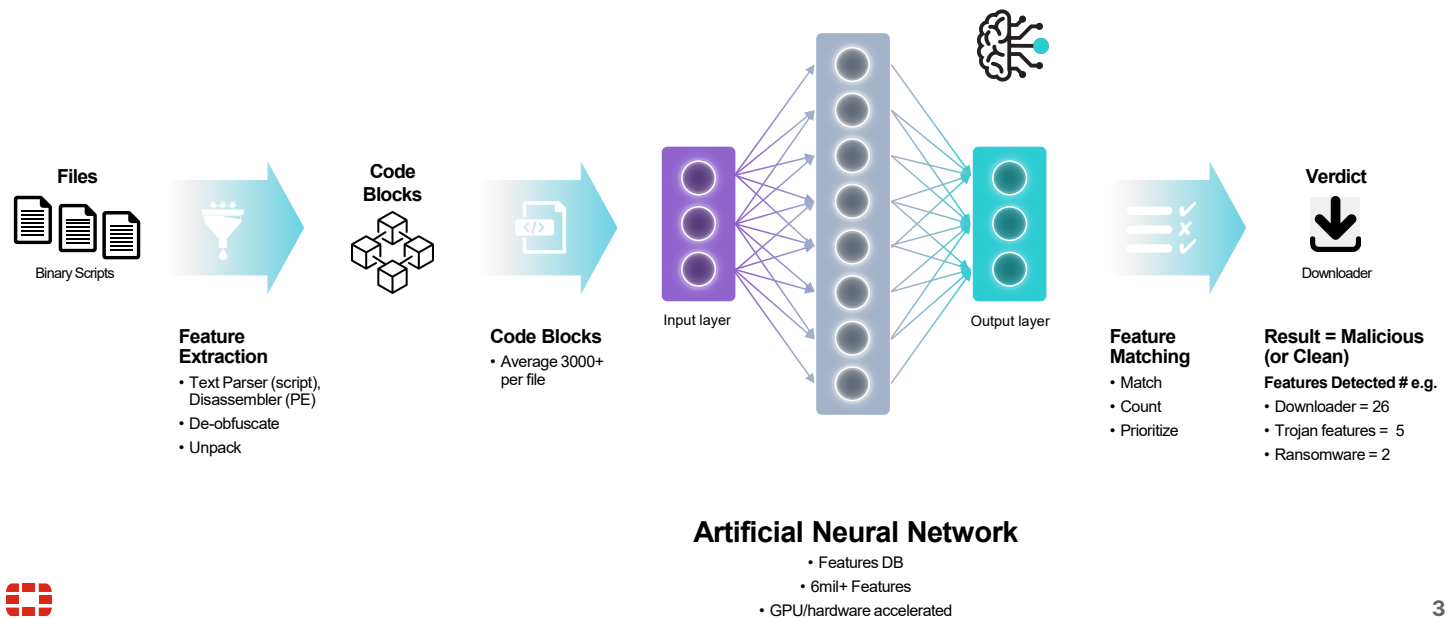
ML-based Traffic Profiling and Malware Detection

Carefully crafted cyber threats designed to bypass your existing security controls through the camouflage with malware detection.

Features	FortiNDR On Premises
Deployment / Data Location	On Premises
Suitable Use	OT, Air-gapped, Large SOC
Centralized Management	Standalone, Center and Sensors mode (up to 20 sensors)*
Sensors, Center, and Standalone Options	Sensor: FortiNDR-1000F, VM16 and VM32 Center Hardware: FortiNDR-3500F, FortiNDR VM for Central Management Standalone: FortiNDR-1000F, VM 16, VM32, and FortiNDR 3500F
Response Integration	FortiGate, FortiSwitch, FortiNAC quarantine, Third party API calls FortiAnalyzer, FortiSIEM, and FortiSOAR
Malware Detection	Antivirus engine and patented Artificial Neural Network (ANN)
Detections and Device Enrichment	Netflow Ingestion and AD Integration
Retention	Throughput and Disk Dependent

* For more than 20 sensors please consult with Fortinet consulting systems engineer team.

FortiNDR Advanced Malware Detection by ANN



Specifications

Category	FortiNDR 1000F	FortiNDR 3500F	FortiNDR VM 16	FortiNDR VM 32	FortiNDR VM Central Management
Deployment					
Sniffer / SPAN / 802.1q support	☑	☑	☑	☑	—
Deployment Mode	Standalone, Sensor	Standalone, Center	Standalone, Sensor	Standalone, Sensor	Center
Sensors Managed *	—	up to 20	—	—	Up to 20
Fortinet Security Fabric Integration (such as FortiGate, FortiSandbox) ¹	☑	☑	☑	☑	—
Hypervisor Support	—	—	ESXi 6.7 U2+, KVM	ESXi 6.7 U2+, KVM	KVM, ESXi 6.7 U2+
Hardware Specifications					
Form Factor	2 RU Rackmount	2 RU Rackmount	—	—	—
Total Interfaces	2x 10/100/1000 RJ45 ports, 4x 10G SFP+, 1x RJ45 console	4x 10GbE SFP+, 2x 10GE Copper (10/100/1000), 2x 1G Copper, 1x DB9 Console	5x virtual interfaces	5x virtual interfaces	5x virtual Interfaces
Sniffer/Capture Interfaces ²	2 (2 x Fiber 10G SFP+)	5 (1 x Copper 10G, 4x 10G Fiber SFP+)	2 x vNIC	2 x vNIC	—
Transceivers Included	purchase separately ²	purchase separately ²	—	—	—
Storage Capacity	2x 7.68 TB (RAID 1) total 7.68 TB (RAID 1)	8x 3.84TB SSD, total 15.36 TB (RAID 10)	1-8TB	1-8TB	1-20TB
Default RAID level (RAID software)	1	10	Hypervisor dependent	Hypervisor dependent	Hypervisor dependent
Removable Hard Drives	☑	☑	—	—	—
Redundant Hot Swappable Power Supplies	☑	☑	—	—	—
Custom GPUs for ANN Acceleration	—	☑	—	—	—
Technical Specifications					
vCPU Support (Minimum / Recommended)	—	—	16/16	32/32	48/64
Memory Support (Minimum / Recommended)	—	—	128 GB (minimum)	256 GB (minimum)	384 GB / 512 GB
Recommended Storage	—	—	1 TB to 8 TB	1 TB to 8 TB	15 TB / 20 TB
System Performance					
NDR Sniffer Throughput**					
HTTP (single/dual port)	10/20 Gbps	10/20 Gbps	6 Gbps (single port)	10 Gbps (single port)	—
Enterprise Mix (single/dual port)	10/20 Gbps	9.5/13 Gbps	4 Gbps (single port)	10 Gbps (single port)	—
Netflows (flows/second)	100k	100k	35k	100k	—
Malware Analysis Throughput (files per hour) ³	170K	130K	40K	120K	—
Malware Classification	26	26	26	26	—

* For deployment more than 20 please consult Fortinet system engineer team.

** The FNDR VM16 and VM32 were tested on DELL PowerEdge R650 (CPU Intel(R) Xeon(R) Platinum 8380 CPU @ 2.30GHz, 256G memory), Tested with FortiNDR 7.4.1 running on VMware vSphere ESXi VMware 8.0.1.

- For full list of Fortinet Fabric integration, please refer to Release Notes for details.
- If copper on FNR-1000F is required (e.g. for mgmt or sniffer), customer can use 1G with Fortinet FN-TRAN-GC. If 10G copper is required on FNR-1000F, customer will need to purchase E10GSFPT from <https://www.fs.com/products/89577.html>. Fortinet FN-TRAN-SFP+SR and FN-TRAN-SFP+LR are also supported on both NDR-1000F and NDR-3500F platforms.
- Combined real world throughput based on 10:1 Non-PE/PE files.



Hardware Specifications

Please click [here](#) for hardware quick start guide.

Category	FortiNDR 1000F	FortiNDR 3500F
Dimensions		
Height x Width x Length (mm)	88.9 mm x 444.5 mm x 574.04 mm	86.8 mm x 482 mm (w/handle) x 751.34 mm (w/bezel) 86.8 mm x 434 mm (w/o handle)x 737.5 mm (w/o bezel)
Weight		
Weight	34.6 lbs (16 kg)	68.34 lbs (31 kg)
Environment		
AC Power Supply	100-240 VAC, 60-50 Hz	100-240 VAC, 60-50 Hz
Power Consumption (Average/ Maximum)	163 W (idle) / 345 W (full loading)	1390 W / 1668 W
Heat Dissipation	1207.5 BTU/h	6824 BTU/h
Operating Temperature	0°C to 40°C (32°F to 104°F) with no direct sunlight on the equipment	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment
Storage Temperature	-20°C to 70°C (-4°F to 158°F)	-40°C to 65°C (-40°F to 149°F)
Humidity	Storage: 5% to 90% non-condensing	Storage: 5% to 95% RH with 33°C (91°F) maximum dew point. Atmosphere must be non-condensing at all times. Operation: 10% to 80% relative humidity with 29°C (84.2°F)
Operating Altitude		
Operating Altitude	Up to 16 404 ft (5000 m)	Up to 7400 ft (2250 m)
Compliance		
Safety Certifications	FCC Part 15 Class A, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB



Ordering Information

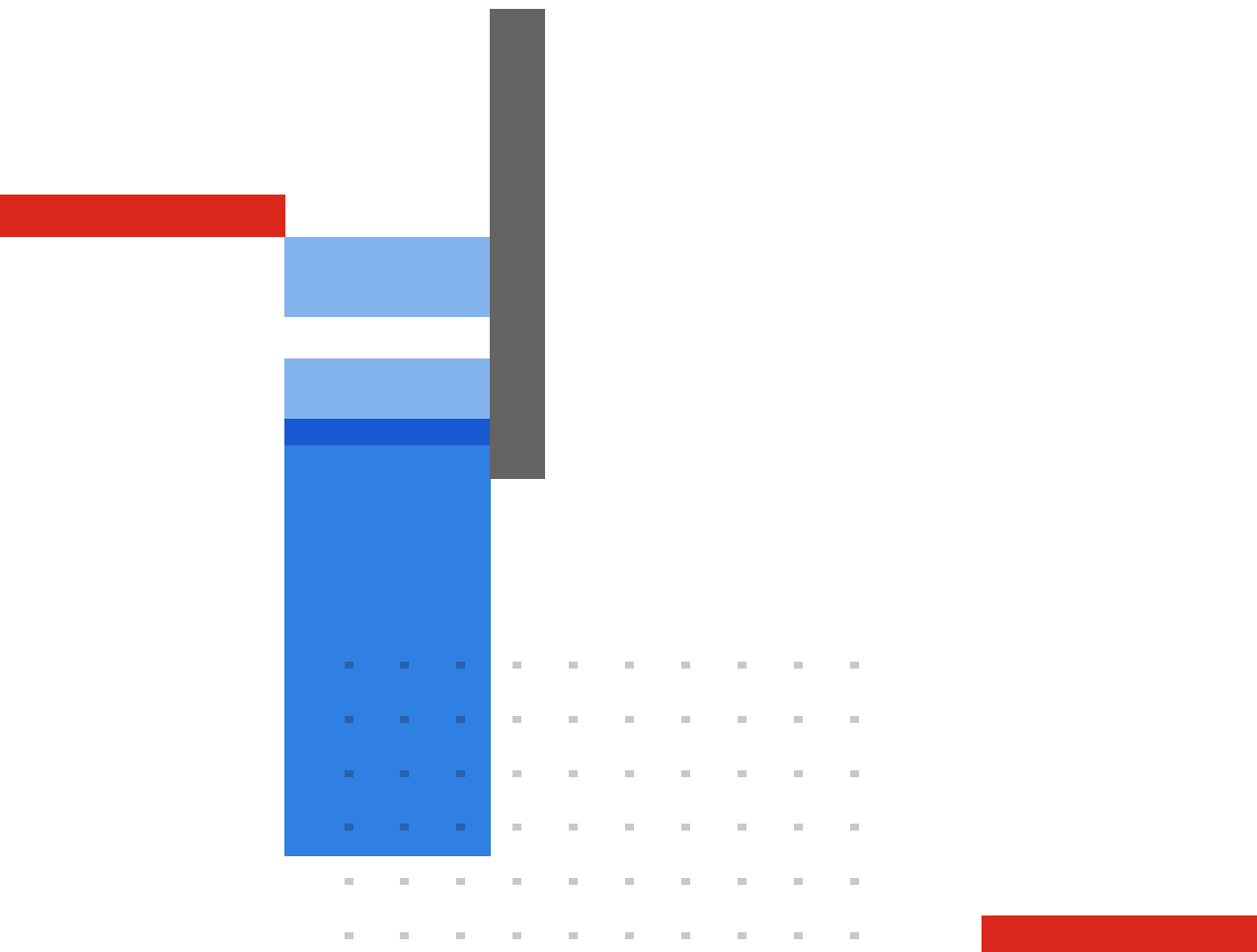
Please click [here](#) for the FortiNDR Ordering Guide.

PRODUCT	SKU	DESCRIPTION
Devices		
FortiNDR-1000F	FNR-1000F	Appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 4x 10GbE SFP+, 2 x 1Gigabit Ethernet connection (management). Netflow order separately.
FortiNDR-1000F Hardware Bundle	FNR-1000F-BDL-331-DD	FortiNDR-1000F Hardware plus FortiCare Premium, with NDR and ANN engine updates and baseline. FortiNDR-1000F appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 4x 10GbE SFP+, 2x 10Gb GE Copper (supports 10/1000/10000 without transceivers), 2x 1 Gigabit Ethernet connection (management). Netflow order separately.
Netflow for FortiNDR-1000F	FC-10-AI1KF-588-02-DD	Netflow Support for FortiNDR-1000F.
SCADA for FortiNDR-1000F	FC-10-AI1KF-723-02-DD	SCADA Support for FortiNDR-1000F.
FortiNDR-1000F renewal	FC-10-AI1KF-331-02-DD	FortiCare Premium with NDR and ANN engine updates and baseline.
FortiNDR 3500F	FNR-3500F	FortiNDR-3500F appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 4x 10GbE SFP+, 2x 10Gb GE Copper (supports 10/1000/10 000 without transceivers), 2x 1 Gigabit Ethernet connection (management). Transceivers order separately.
FortiNDR-3500F Hardware Bundle	FNR-3500F-BDL-331-DD	FortiNDR-3500F bundle - Hardware plus 24x7 FortiCare and NDR and ANN updates and baseline.
Netflow for FortiNDR-3500F	FC-10-AI3K5-588-02-DD	Netflow Support for FortiNDR-3500F.
SCADA for FortiNDR-3500F	FC-10-AI3K5-723-02-DD	SCADA Support for FortiNDR-3500F.
Virtual Machines		
FortiNDR-VM16 Subscription License with Bundle	FC3-10-AIVMS-461-02-DD	Subscriptions license for FortiNDR-VM (16 CPU) with 24x7 FortiCare plus NDR and ANN updates and baseline.
Netflow for VM16	FC3-10-AIVMS-588-02-DD	Netflow Support for FortiNDR-VM16.
SCADA for VM16	FC3-10-AIVMS-723-02-DD	SCADA Support for FortiNDR-VM16.
FortiNDR-VM32 Subscription License with Bundle	FC4-10-AIVMS-461-02-DD	Subscriptions license for FortiNDR-VM (32 CPU) with 24x7 FortiCare plus NDR and ANN updates and baseline.
Netflow for VM32	FC4-10-AIVMS-588-02-DD	Netflow Support for FortiNDR-VM32.
SCADA for VM32	FC4-10-AIVMS-723-02-DD	SCADA Support for FortiNDR-VM32.
FortiCare and Updates	FC-10-AI3K5-331-02-DD	24x7 FortiCare plus FortiGuard Neural Networks engine updates and baseline.
FortiNDR-VM Central Management Subscription	FC1-10-AIVMC-757-02-DD	FortiNDR Central Management Subscription License, managed up to 10 FortiNDR on-premise appliance/VM deployment, includes FortiCare premium.
	FC5-10-AIVMC-757-02-DD	FortiNDR Central Management Subscription License, managed up to unlimited number of FortiNDR on-premise appliance/VM deployment, includes FortiCare premium.
Accessories		
3.84TB 2.5 inch SATA SSD with Tray	SP-DFAI-3T	3.84TB 2.5 in. SATA SSD with tray for FortiNDR-3500F.
10GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10GE SFP+ transceiver module, 10km long range for systems with SFP+ and SFP/SFP+ slots.
10GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots.
10GE copper SFP+ RJ45 Transceiver (30m range) *see pg 5	FN-TRAN-SFP+GC	10GE copper SFP+ RJ45 transceiver module (30m range) for systems with SFP+ slots.
1GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1GE SFP RJ45 transceiver module for systems with SFP and SFP/SFP+ slots.



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

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.