

FortiNDR and FortiNDR Cloud



Highlights

- Detect and respond to cyberattacks with powerful AI
- Discover detection aggregating metadata
- Leverage turnkey security where legacy detection fails
- Fill gap in SOC skills and resource shortages

Network Detection and Response

FortiNDR and FortiNDR Cloud (aka ThreatINSIGHT) represent the future of AI-driven breach protection technology, designed for short-staffed Security Operation Center (SOC) teams to defend against various threats including advanced persistent threats through trained Virtual Security Analyst™ and “Guided SaaS” that helps you identify, classify, and respond to threats including those well camouflaged. The use of metadata in threat detection is essential in modern SOC. Supervised and unsupervised ML can be applied to metadata, especially in east-west data in datacenters to identify threats. 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



Cloud
SaaS



Public
Cloud

Key Features¹

- Detect network anomalies where traditional security solutions fail
- Investigate threats with historical trends and 365 days of data
- Hunt adversaries with guided playbooks
- Automate and manually respond for quarantine and control
- Mimic experienced security analyst for outbreak, anomalies, and malware detection, processing large volume of network data
- Reduce malware detection and investigation time from minutes to seconds²
- Provide on-premises learning to reduce false positives by analyzing organizational-specific traffic and adapting to newly disguised threats
- Integrate into Fortinet's Security Fabric by uniting with FortiGates and others to automatically quarantine attacks
- Analyze zero days scientifically including fileless threats and classify them into 20+ malware attack scenarios

¹ Please see feature comparison between FortiNDR and FortiNDR Cloud next page.

² Patent pending #U.S.16/053,479

Basic Competencies

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™**, as well as **Guided** Technical Success Managers (TSM) with FortiNDR Cloud

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



Highlights

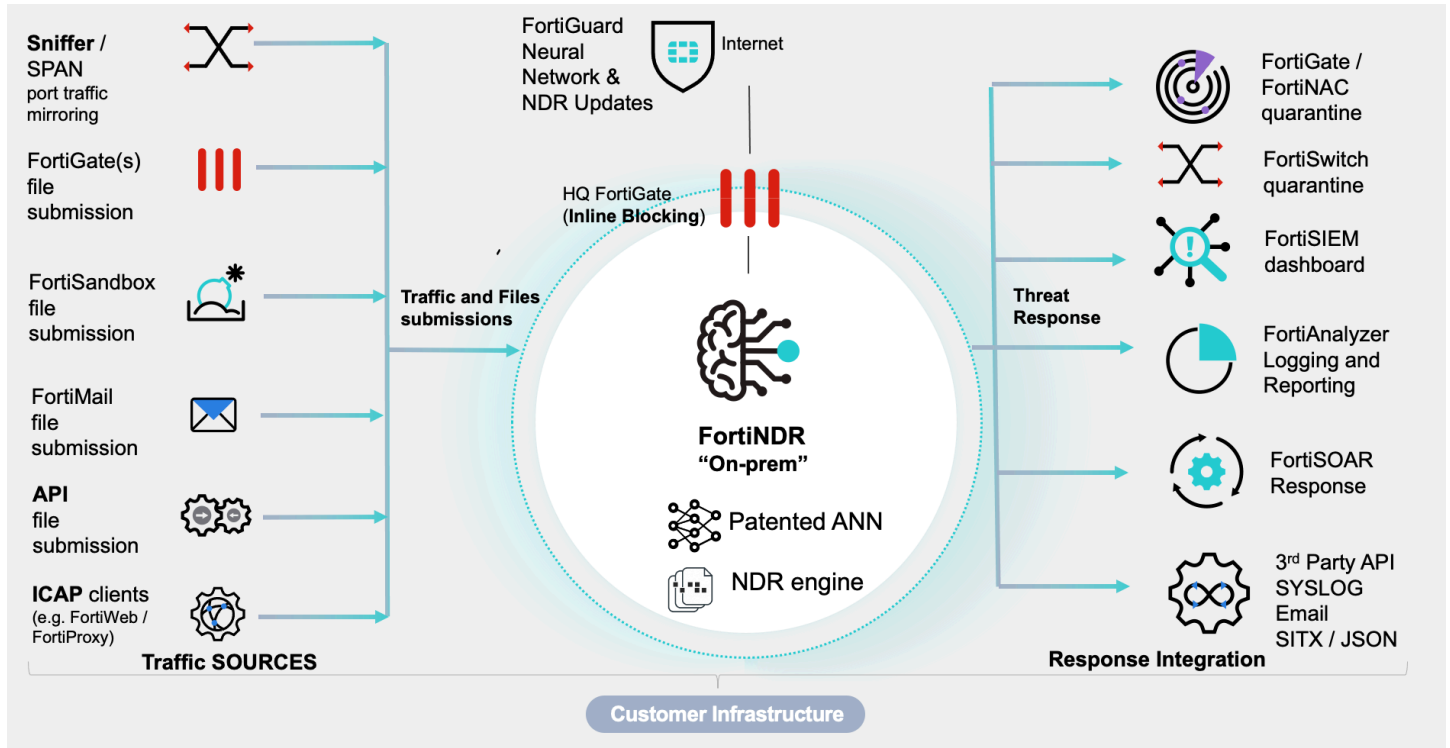
Features	FortiNDR (HW/VM)	FortiNDR Cloud
Deployment	On-premise	SaaS
Security Analyst	Virtual Security Analyst™	Guided-SaaS with TSM (Technical Success Manager)
Data Storage Location	On-prem	Cloud-based (US)
Data Retention	Throughput/Disk-dependent	365 Days
Investigation / Threat Hunting	Outbreak Search	Guided Playbooks and Parallel Hunting
Netflow/IPFIX Support	Yes	—
High Throughput Malware Scan / NFS Scanning	Yes ANN ¹ with On-prem Learning	Hash Lookup
MITRE ATT&CK Framework Mapping	Malware mapped to MITRE ATT&CK Framework	Detections mapped to MITRE ATT&CK Framework
Response Integration	Fortinet Security Fabric Third-party API (Rest) MetaStream with Signals	
Sensors	Hardware: FortiNDR-1000F, FortiNDR-3500F VM16 / VM32 (ESXi / KVM) AWS / Azure / GCP / Alibaba	Hardware: FortiNDR Cloud-900F (Large sensor) Hardware: FortiNDR Cloud-500F (Small sensor) Virtual Sensors (AWS / Azure / ESXi / KVM)
FortiGuard Labs Threat Research	☑	☑

1. Artificial Neural Networks

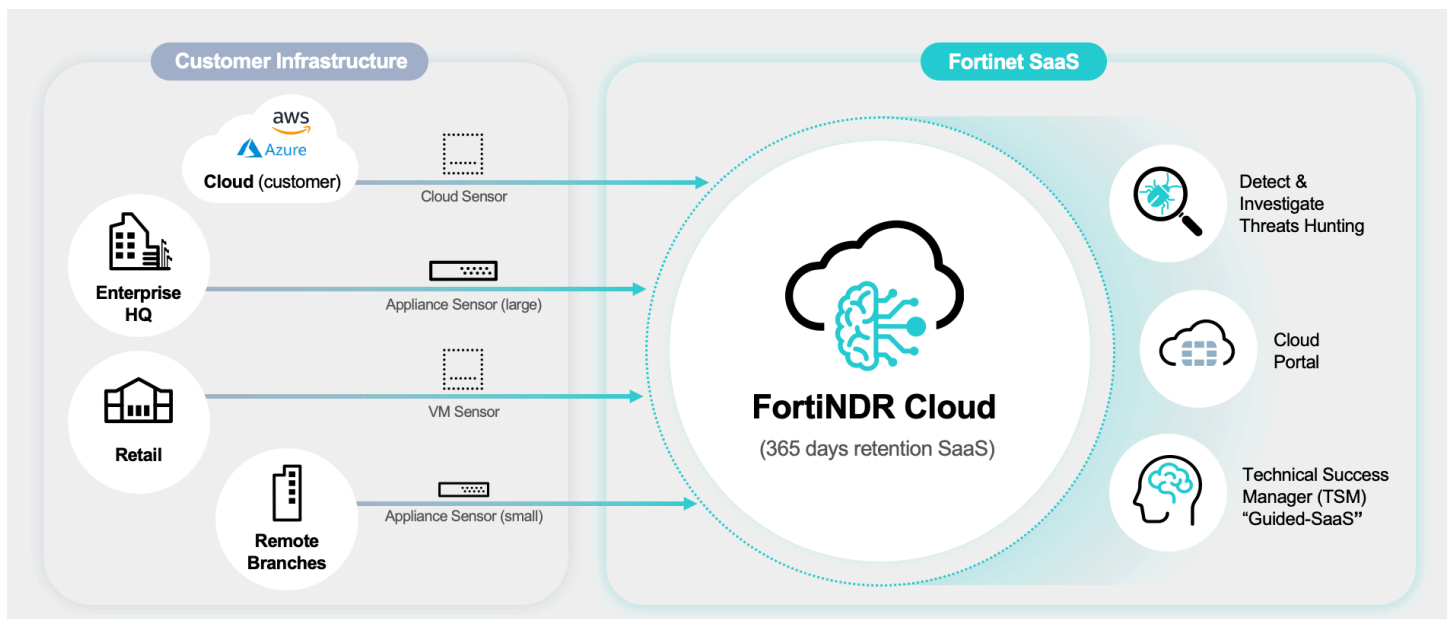


Deployment

FortiNDR (on prem) Architecture and Integration



FortiNDR Cloud Architecture and Deployment



Specifications

Category	FortiNDR-1000F	FortiNDR-3500F	FNDR VM 16	FNDR VM 32	FNDR Cloud 500F small sensor	FNDR Cloud 900F large sensor	FNDR Cloud Virtual Sensors
Deployment							
Sniffer / SPAN / 802.1q support	☑	☑	☑	☑	☑	☑	☑
Cloud based sensors + SaaS portal	—	—	—	—	☑	☑	☑
Integrated (with fabric devices) and ICAP	☑	☑	☑	☑	—	—	—
Hypervisor Support	—	—	ESXi 6.7 U2+, KVM	ESXi 6.7 U2+, KVM	—	—	ESXi6.7 U2+, KVM
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	4x virtual interfaces	4x virtual interfaces	1x 1G Copper, 2x 10G SFP+, 2x 10G Copper	1x 1G Copper, 2x 10G SFP+, 2x 10G Copper	1 mgmt + min 1 TAP
Sniffer Interfaces	3 (3 x Fiber 10G SFP+)*	5 (1 x Copper 10G, 4 x 10G Fiber SFP+)*	1 x vNIC	1 x vNIC	5 (1 x 1G Copper, 2 x 10G SFP+, 2 x 10G Copper)	5 (1 x 1G Copper, 2 x 10G SFP+, 2 x 10G Copper)	min 1 x vNIC max 3 x vNIC
Transceivers Included	purchase separately ²	purchase separately	—	—	2x 10G multimode	4x 10G multimode	—
Storage Capacity	2 x 7.68 TB (RAID 1) total 7.68 TB (RAID 1)	8 x 3.84TB SSD, total 15.36 TB (RAID 10)	1-8TB	1-8TB	890 GB	890 GB	100 (min) - 300 GB (recommended)
Default RAID level (RAID software)	1	10	Hypervisor dependent	Hypervisor dependent	10	10	Hypervisor dependent
Removable Hard Drives	☑	☑	—	—	Yes	Yes	—
Redundant Hot Swappable Power Supplies	☑	☑	—	—	Yes	Yes	—
Custom GPUs for ANN Acceleration	—	☑	—	—	—	—	—
Technical Specifications							
vCPU Support (Recommended)	—	—	16	32	—	—	16
Memory Support (Minimum / Recommended)	—	—	32 GB / 128 GB	64 GB / 256 GB	—	—	16 GB / 32 GB
Recommended Storage	—	—	1 TB to 8 TB	1 TB to 8 TB	—	—	—
System Performance							
NDR Sniffer Throughput	10 Gbps / 10 Gbps (HTTP/enterprise mix) - single port sniffer 20 Gbps / 20 Gbps (HTTP/ P/enterprise mix) - dual port sniffer	10 Gbps/ 9.5 Gbps (HTTP/enterprise mix) - single port sniffer 20 Gbps/ 13 Gbps (HTTP/enterprise mix) - dual port sniffer	Hypervisor dependent	Hypervisor dependent	2 Gbps (metadata processing) across all ports	10 Gbps (metadata processing) across all ports	Hypervisor dependent
Malware Analysis Throughput (files per hour) ¹	170K files per hour	130K files per hour	40K	80K	Hash lookup (VT) on SaaS	Hash lookup (VT) on SaaS	Hash lookup (VT) on SaaS
Malware Classification	26 categories	26 categories	26 categories	26 categories	—	—	—

1) Combined real world throughput based on 10:1 Non-PE/PE files.

2) 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 E10GSFP 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.



Specifications

Category	FortiNDR-1000F	FortiNDR-3500F	FNDR VM 16	FNDR VM 32	FNDR Cloud 500F small sensor	FNDR Cloud 900F large sensor	FNDR Cloud Virtual Sensors
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)	—	—	42.8 mm. x 482 mm (w/ handle) x 757.75 mm (w/ bezel) 42.8mm x 434 mm (w/o handle) x 743.91 mm (w/o Bezel)	42.8 mm. x 482 mm (w/ handle) x 757.75 mm (w/ bezel) 42.8mm x 434 mm (w/o handle) x 743.91 mm (w/o Bezel)	—
Weight	34.6 lbs (16 kg)	68.34 lbs (31 kg)	—	—	25.9 kg	25.9 kg	—
Environment							
AC Power Supply	100-240 VAC, 60-50 Hz	100-240 VAC, 60-50 Hz	—	—	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	—	—	276 W / 390 W	409 W / 619 W	—
Heat Dissipation	1207.5 BTU/h	6824 BTU/h	—	—	2891 BTU/h	2891 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	—	—	10°C to 35°C (50°F to 95°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)	—	—	-40°C to 65°C (-40°F to 149°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)	—	—	Storage: 5% to 95% RH with 33°C (91°F) maximum dew point. Atmosphere must be non-condensing at all times. Operating: 10% to 80% relative humidity with 29°C (84.2°F) maximum dew point.	Storage: 5% to 95% RH with 33°C (91°F) maximum dew point. Atmosphere must be non-condensing at all times. Operating: 10% to 80% relative humidity with 29°C (84.2°F) maximum dew point.	—
Operating Altitude	Up to 16 404 ft (5000 m)	Up to 7400 ft (2250 m)	—	—	Up to 10 000 ft (3048 m)	Up to 10 000 ft (3048 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	—	—	FCC, ISSED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB	FCC, ISSED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB	—



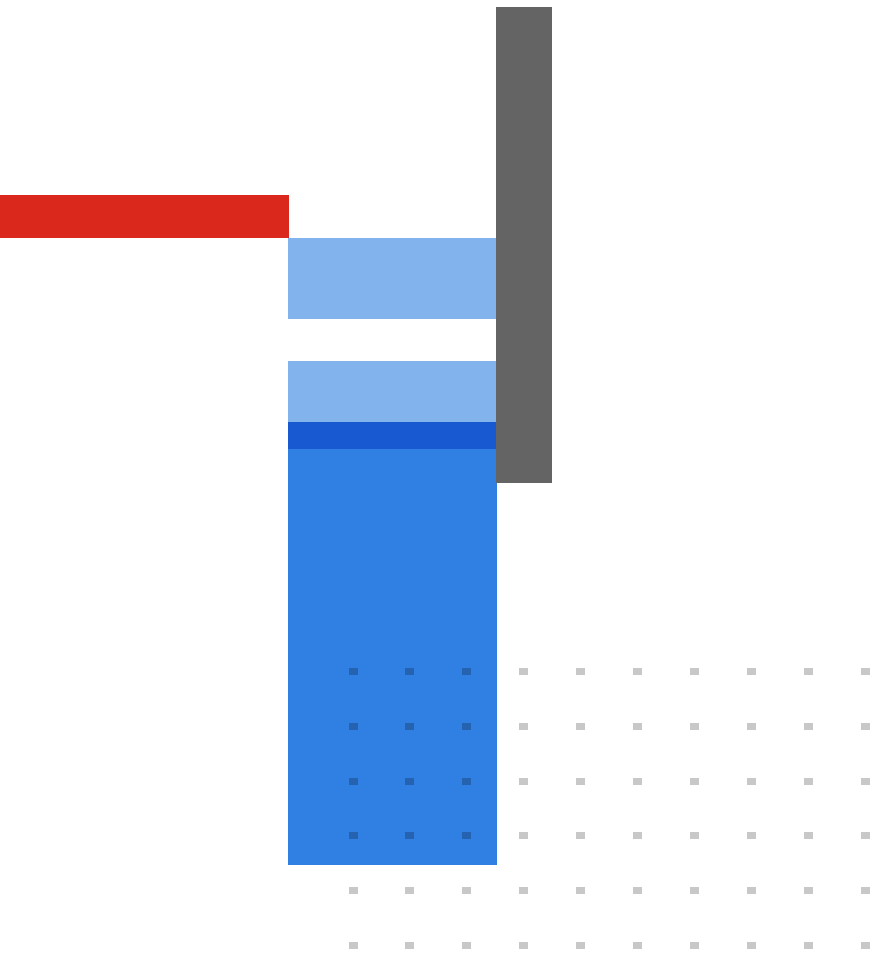
Ordering Information

FORTINDR APPLIANCE AND VM		
Product	SKU	Description
FortiNDR-1000F	FNR-1000F	Appliance for Network Anomalies and Oday/Malware Detection, based on Artificial Neural Network (ANN) technology. 4x 10GbE SFP+, 2 x 1Gigabit Ethernet connection (management). Netflow order separately.
Netflow for FortiNDR-1000F	FC-10-AI1KF-588-02-DD	Netflow Support for FortiNDR-1000F.
FortiNDR-1000F Hardware Bundle	FNR-1000F-BDL-331-DD	FortiNDR-1000F Hardware plus FortiCare Premium, with NDR and ANN engine updates & baseline. FortiNDR-1000F appliance for Network Anomalies and Oday/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.
FortiNDR-1000F renewal	FC-10-AI1KF-331-02-DD	FortiCare Premium with NDR and ANN engine updates & baseline.
Product	SKU	Description
FortiNDR 3500F	FNR-3500F	FortiNDR-3500F appliance for Network Anomalies and Oday/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.
Netflow for FortiNDR-3500F	FC-10-AI3K5-588-02-DD	Netflow Support for FortiNDR-3500F.
FortiNDR-3500F Hardware Bundle	FNR-3500F-BDL-331-DD	FortiNDR-3500F bundle - Hardware plus 24x7 FortiCare and NDR and ANN updates and baseline.
Product	SKU	Description
FortiNDR-VM 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.
	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 VM16	FC3-10-AIVMS-588-02-DD	Netflow Support for FortiNDR-VM16.
Netflow for VM32	FC4-10-AIVMS-588-02-DD	Netflow Support for FortiNDR-VM32.
FortiCare and Updates	FC-10-AI3K5-331-02-DD	24x7 FortiCare plus FortiGuard Neural Networks engine updates and baseline.
FORTINDR ACCESSORIES		
Product	SKU	Description
3.84TB 2.5" SATA SSD with Tray	SP-DFAI-3T	3.84TB 2.5" 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.
FORTINDR CLOUD		
Product	SKU	Description
FortiNDRCloud-SAAS Services	FC1-10-NDRCL-667-02-12	Annual Subscription license for FortiNDR Cloud Guided-SaaS Platform with Detections, Investigations, Playbooks, and Reports at 1 Gbps of metered usage. Includes FortiCare premium. Does not include physical sensors.
True Up Usage	NDRC-TRUEUP-1MTH	Throughput True-up SKU for traffic overages in FortiNDR Cloud for 1 Gbps of metered usage.
FortiNDRCloud-500F	FNRC-500F	FortiNDRCloud 500F (small) physical sensor to deliver data to FortiNDR Cloud SaaS Platform. Hardware Only. 1U with 2 x Copper / 2 x Fiber SFP+. Must purchase support. Ship with 2 x 10G multimode transceivers.
Small Sensor (500F) Licence and Support	FC-10-NDR5F-247-02-DD	Annual license for support for FNRC-500F (small) sensor and forwarding traffic to the FortiNDR Cloud SaaS Platform, includes FortiCare premium.
FortiNDRCloud-900F	FNRC-900F	FortiNDRCloud 900F (large) physical sensor to deliver data to FortiNDR Cloud SaaS Platform. Hardware Only. 1U with 2 x Copper / 2 x Fiber SFP+. Must purchase support. Ship with 4 x 10G multimode transceivers
Large Sensor (900F) Licence and Support	FC-10-NDR9F-247-02-DD	Annual license for support for FNRC-900F (large) sensor and forwarding traffic to the FortiNDR Cloud SaaS Platform, includes FortiCare premium.

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](#).





FORTINET

www.fortinet.com

Copyright © 2023 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.

May 15, 2023

FNDR-DAT-R11-20230515