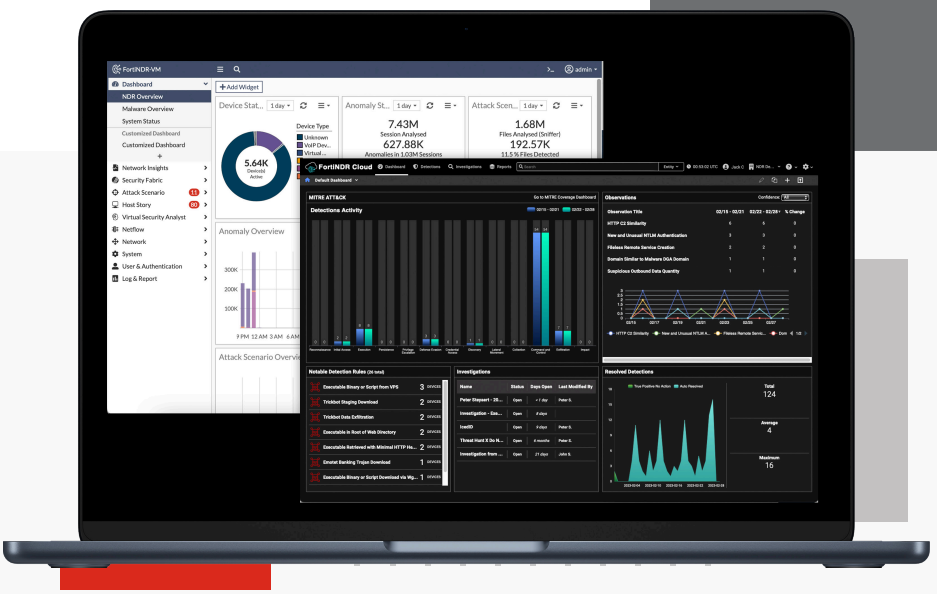
# FortiNDR and FortiNDR Cloud



## 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 Features[1]

- 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 seconds[2]
- 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

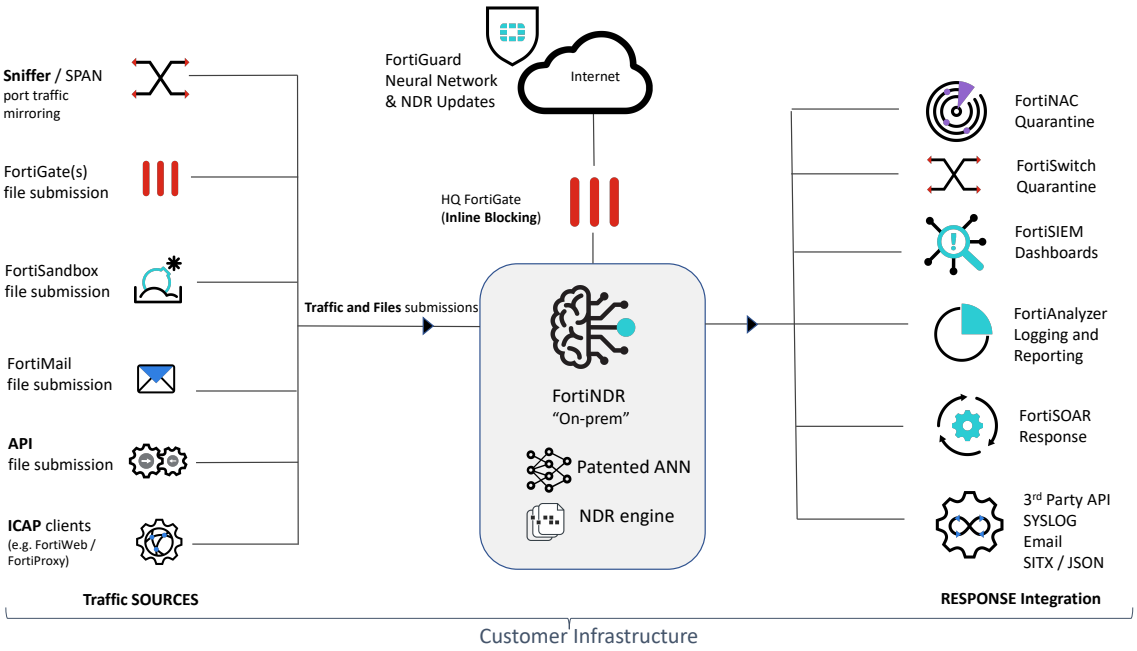
**ML-based Traffic Profiling and Malware Detection**
Carefully crafted cyber threats designed to bypass your existing security controls through the camouflage with malware detection

# Highlights

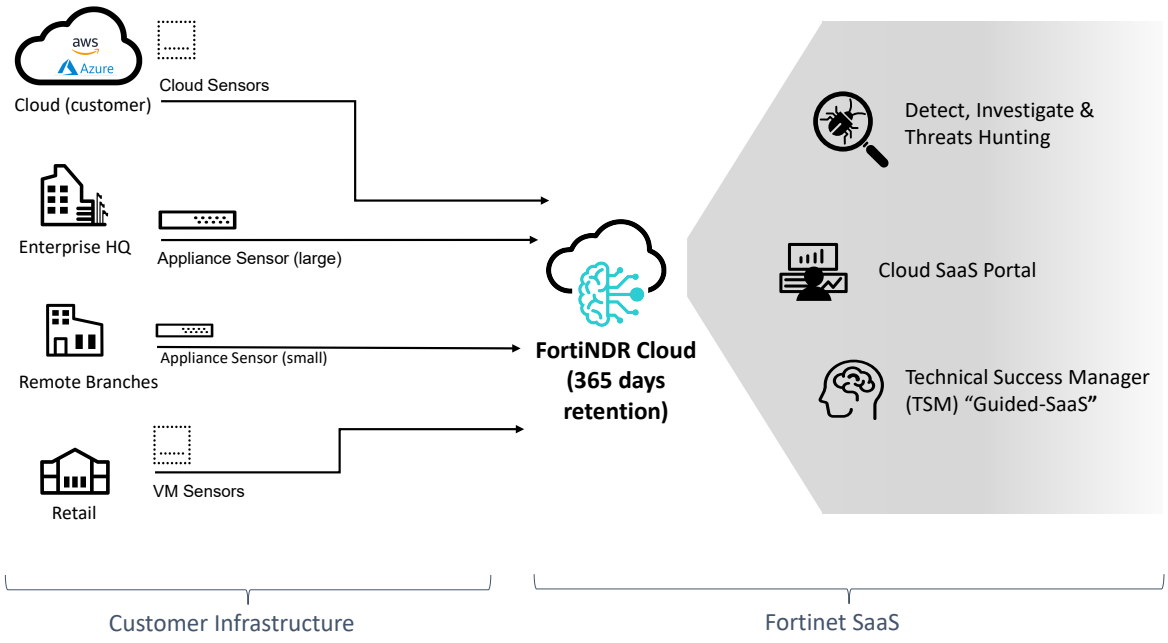
| Features | FortiNDR (on prem) | FortiNDR Cloud (aka ThreatInsight) |
|---|---|---|
| **Deployment** | On-prem sensors with detection | SaaS portal with sensors |
| **Security Analyst** | Virtual Security Analyst™ (Software Feature) | "Guided" SaaS with TSM (Technical Success Manager) |
| **Response Integration** | FortiGate (FortiAnalyzer Reporting)<br>FortiNAC / FortiSIEM / FortiSOAR<br>FortiSwitch<br>Third Party API (REST) | Third Party via API / MetaStream e.g. Crowdstrike, Splunk, Qradar, PAN XSoar |
| **Sensors** | Hardware - FortiNDR-3500F<br>VM16 / VM32 (ESXi / KVM)<br>AWS / Azure / GCP / Alibaba (full featured solution) | Hardware - FortiNDRCloud-900F (Large sensor)<br>Hardware - FortiiNDRCloud-500F (Small sensor)<br>Virtual sensors (ESXi / KVM)<br>AWS / Azure (sensors only) |
| **Security Research** | FortiGuard ML/AI/ANN | FortiGuard Applied Threat Research |
| **Data Storage Location** | Onsite | Cloud based (US) |
| **Retention** | Depends on throughput/disks | 365 days |
| **Investigation / Threat Hunt** | Limited | Full featured with user defined queries |
| **MITRE ATT&CK support** | Malware only | Threats/Detection with MITRE widgets<br>MITRE map for all detections |
| **Central Management** | Centralized logging and reporting - FortiAnalyzer | Centralized portal for log/report/investigations |
| **Distributed deployment** | Limited to appliance(s) and/or VMs | Easy to deploy additional sensors<br>Cloud Scale (storage) |
| **Netflow/SFlow/IPFIX support** | Yes | Not available |
| **High Throughput Malware Scan / NFS Scanning** | Yes, malware classification with On-prem learning | Not available (In-cloud Hash lookup on VT) |

# Deployment

**FortiNDR (on prem) Architecture and Integration**




**FortiNDR Cloud Architecture and Deployment**



# Specifications

| Category | 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** | ✓ | ✓ | ✓ | — | — | — |
| **vCPU / memory (min/max)** | — | 128 GB | 256 GB | — | — | Min 16 / 32GB |
| **Hypervisor Support** | — | ESXi 6.7 U2+, KVM | ESXi 6.7 U2+, KVM | — | — | — |
| **Hardware Specifications** | | | | | | |
| **Form Factor** | 2 RU Rackmount | — | — | — | — | — |
| **Total Interfaces** | 4× 10GbE SFP+, 2× 10GE Copper (10/100/1000), 2× 1G Copper, 1x DB9 Console | 4x virtual interfaces | 4x virtual interfaces | 1 mgmt + 5 TAPs | 1 mgmt + 5 TAPs | 1 mgmt + min 1 TAP |
| **Transceivers Included** | purchase separately | — | — | 2× 10G multimode | 4× 10G multimode | — |
| **Storage Capacity** | 8 × 3.84TB SSD, total 15.36 TB (Raid 10) | 1-8TB | 1-8TB | 890 GB | 890 GB | 100 GB min, 300 GB rec |
| **Default RAID level (RAID software)** | 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)** | — | 128 GB / 256 GB | 128 GB / 256 GB | — | — | 32 GB |
| **Recommended Storage** | — | 1 TB to 8 TB | 1 TB to 8 TB | — | — | — |
| **System Performance** | | | | | | |
| **NDR Sniffer Throughput[1]** | 9.5/5Gbps (HTTP/enterprise mix) - single port<br>19Gbps/9Gbps (HTTP/enterprise mix) - dual port sniffer | Hypervisor dependent | Hypervisor dependent | 5 Gbps (metadata processing) | 10 Gbps (metadata processing) | Hypervisor dependent |
| **Malware Analysis Throughput (files per hour)[4]** | 100K 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 | — | — | — |

# Specifications

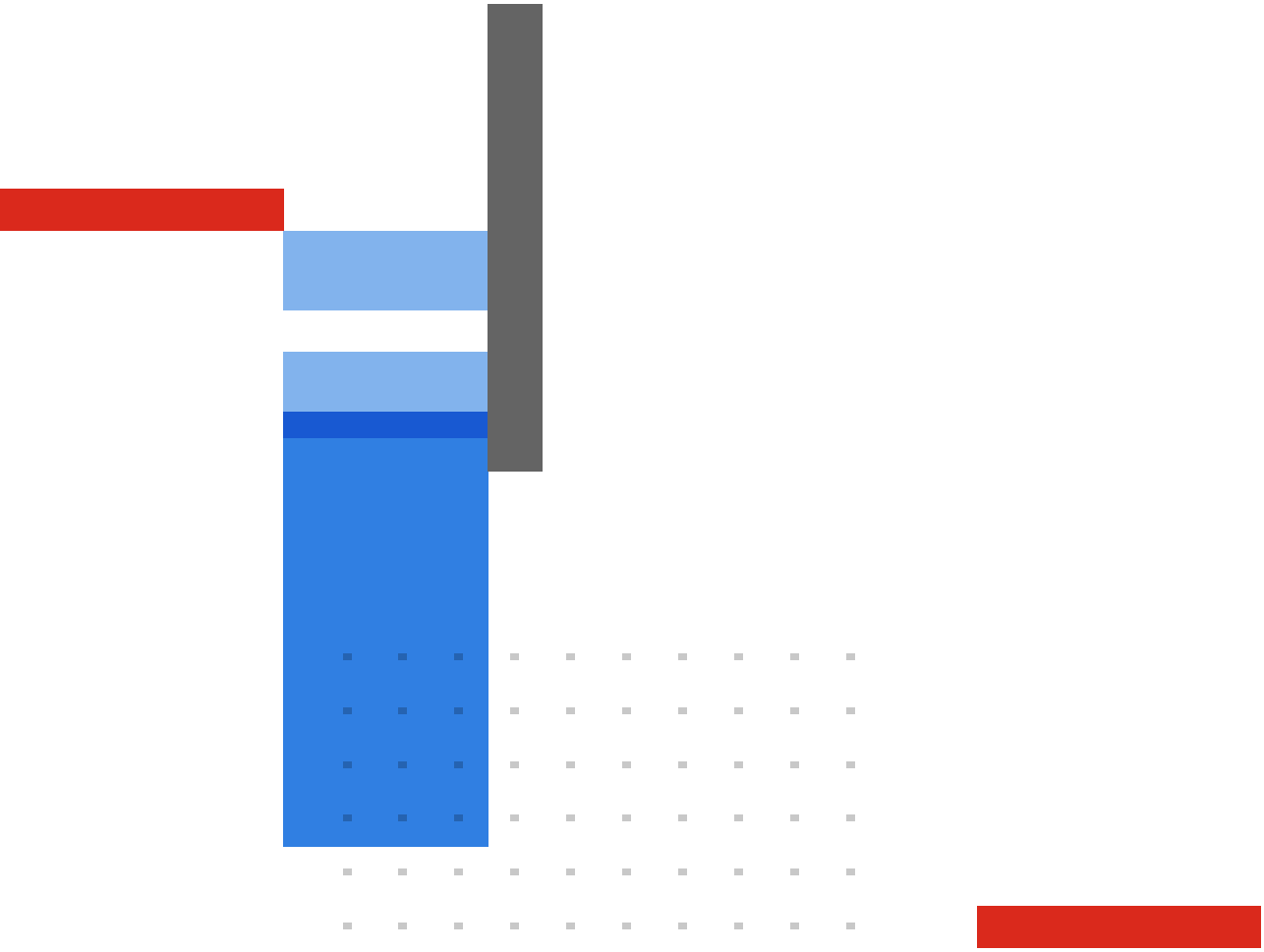
| Category | FortiNDR-3500F | FNDR VM 16 | FNDR VM 32 | FNDR Cloud 500F small sensor | FNDR Cloud 900F large sensor | FNDR Cloud Virtual Sensors |
|---|---|---|---|---|---|---|
| **Dimensions** | | | | | | |
| **Height x Width x Length (mm)** | 86.8mm x 482mm (w/handle) x 751.34mm (w/bezel), 86.8mm x 434mm (w/o handle) x 737.5mm (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** | 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 | — |
| **Power Consumption (Average / Maximum)** | 1390 W / 1668 W | — | — | 276 W / 390 W | 409 W / 619 W | — |
| **Heat Dissipation** | 6824 BTU/h | — | — | 2891 BTU/h | 2891 BTU/h | — |
| **Operating Temperature** | 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** | –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 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 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, RCM, VCCI, CE, UL/cUL, CB | — | — | FCC, ISED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB | FCC, ISED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB | — |

# Ordering Information

| FORTINDR APPLIANCE AND VM | | |
|---|---|---|
| **Product** | **SKU** | **Description** |
| **FortiNDR 3500F** | FNR-3500F | FortiNDR-3500F appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 4× 10GbE SFP+, 2× 10Gb GE Copper (supports 10/1000/10 000 without transceivers), 2× 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 24×7 FortiCare and NDR and ANN updates and baseline. |
| **FortiNDR-VM Subscription License with Bundle** | FC3-10-AIVMS-461-02-DD | Subscriptions license for FortiNDR-VM (16 CPU) with 24×7 FortiCare plus NDR and ANN updates and baseline. |
| | FC4-10-AIVMS-461-02-DD | Subscriptions license for FortiNDR-VM (32 CPU) with 24×7 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 | 24×7 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. |
| **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 ussage. 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 × 10G multimode transceivers. |
| **Small Sensor (500F) Licence and Suppport** | 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 × 10G multimode transceivers |
| **Large Sensor (500F) Licence and Suppport** | 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.



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.

March 2, 2023

FNDR-DAT-R05-20230302