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.
### 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
- 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 Premises Deployment

![FortiNDR On Premises Deployment Diagram](image-url)
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.

<table>
<thead>
<tr>
<th>Features</th>
<th>FortiNDR On Premises</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment / Data Location</td>
<td>On Premises</td>
</tr>
<tr>
<td>Suitable Use</td>
<td>OT, Air-gapped, Large SOC</td>
</tr>
<tr>
<td>Centralized Management</td>
<td>Standalone, Center and Sensors mode (up to 20 sensors)</td>
</tr>
<tr>
<td>Sensors, Center, and Standalone Options</td>
<td>Sensor: FortiNDR-1000F, VM16 and VM32</td>
</tr>
<tr>
<td></td>
<td>Center Hardware: FortiNDR-3500F</td>
</tr>
<tr>
<td></td>
<td>Standalone: FortiNDR-1000F, VM16, VM32, and FortiNDR 3500F</td>
</tr>
<tr>
<td>Response Integration</td>
<td>FortiGate, FortiSwitch, FortiNAC quarantine, Third party API</td>
</tr>
<tr>
<td></td>
<td>calls</td>
</tr>
<tr>
<td></td>
<td>FortiAnalyzer, FortI SIEM, and FortISOAR</td>
</tr>
<tr>
<td>Malware Detection</td>
<td>Antivirus engine and patented Artificial Neural Network (ANN)</td>
</tr>
<tr>
<td>Detections and Device Enrichment</td>
<td>Netflow Ingestion and AD Integration</td>
</tr>
<tr>
<td>Retention</td>
<td>Throughput and Disk Dependent</td>
</tr>
</tbody>
</table>

FortiNDR Advanced Malware Detection by ANN

Artificial Neural Network
- Features DB
- 6mil+ Features
- GPU/hardware accelerated

Facts
- Features DB
- 6mil+ Features
- GPU/hardware accelerated
## Specifications

<table>
<thead>
<tr>
<th>Category</th>
<th>FortiNDR-1000F</th>
<th>FortiNDR-3500F</th>
<th>FNDR VM 16</th>
<th>FNDR VM 32</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deployment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sniffer / SPAN / 802.1q support</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Deployment Mode</strong></td>
<td>Standalone, Sensor</td>
<td>Standalone, Center</td>
<td>Standalone, Sensor</td>
<td>Standalone, Sensor</td>
</tr>
<tr>
<td>Sensors Managed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fortinet Security Fabric Integration (such as FortiGate, FortiSandBox)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hypervisor Support</strong></td>
<td></td>
<td></td>
<td>ESXi 6.7 U2+, KVM</td>
<td>ESXi 6.7 U2+, KVM</td>
</tr>
<tr>
<td><strong>Hardware Specifications</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Form Factor</td>
<td>2 RU Rackmount</td>
<td>2 RU Rackmount</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Interfaces</strong></td>
<td>2x 10/100/1000 RJ45 ports, 4x 10G SFP+, 1x RJ45 console</td>
<td>4x 10Gbe SFP+, 2x 10GE Copper (10/100/1000), 2x 1G Copper, 1x SFP+ Console</td>
<td>4x virtual interfaces</td>
<td>4x virtual interfaces</td>
</tr>
<tr>
<td>Sniffer/Capture Interfaces²</td>
<td>2 (2 x Fiber 10G SFP+)</td>
<td>5 (1 x Copper 10G, 4 x 10G Fiber SFP+)</td>
<td>2 x vNIC</td>
<td>2 x vNIC</td>
</tr>
<tr>
<td>Transceivers Included</td>
<td>purchase separately²</td>
<td>purchase separately²</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Storage Capacity</strong></td>
<td>2 x 7.68 TB (RAID 1), total 7.68 TB (RAID 1)</td>
<td>8 x 3.84TB SSD, total 15.36 TB (RAID 10)</td>
<td>1-8TB</td>
<td>1-8TB</td>
</tr>
<tr>
<td>Default RAID level (RAID software)</td>
<td>1</td>
<td>10</td>
<td>Hypervisor dependent</td>
<td>Hypervisor dependent</td>
</tr>
<tr>
<td>Removable Hard Drives</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redundant Hot Swappable Power Supplies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom GPUs for ANN Acceleration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Technical Specifications</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCPU Support (Recommended)</td>
<td></td>
<td></td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>Memory Support (Minimum / Recommended)</td>
<td></td>
<td></td>
<td>32 GB / 128 GB</td>
<td>64 GB / 256 GB</td>
</tr>
<tr>
<td>Recommended Storage</td>
<td></td>
<td></td>
<td>1 TB to 8 TB</td>
<td>1 TB to 8 TB</td>
</tr>
<tr>
<td><strong>System Performance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDR Sniffer Throughput</td>
<td>10 Gbps / 10 Gbps (HTTP/enterprise mix) - single port sniffer</td>
<td>10 Gbps / 9.5 Gbps (HTTP/enterprise mix) - single port sniffer</td>
<td>Hypervisor dependent</td>
<td>Hypervisor dependent</td>
</tr>
<tr>
<td>Netflow Flows/Second</td>
<td>70k per sec</td>
<td>70k per sec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware Analysis Throughput (files per hour)³</td>
<td>170K files per hour</td>
<td>130K files per hour</td>
<td>40K</td>
<td>80K</td>
</tr>
<tr>
<td>Malware Classification</td>
<td>26 categories</td>
<td>26 categories</td>
<td>26 categories</td>
<td>26 categories</td>
</tr>
</tbody>
</table>

---

1. For full list of Fortinet Fabric integration, please refer to Release Notes for details.

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+T from [https://www.fs.com/products/89577.html](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.

3. Combined real world throughput based on 10:1 Non-PE/PE files.
# Specifications

<table>
<thead>
<tr>
<th>Category</th>
<th>FortiNDR-1000F</th>
<th>FortiNDR-3500F</th>
<th>FNDR VM 16</th>
<th>FNDR VM 32</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dimensions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height x Width x Length (mm)</td>
<td>86.9 mm x 444.5 mm x 574.04 mm</td>
<td>86.6 mm x 482 mm (w/handle) x 751.34 mm (w/bezel)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>34.6 lbs (16 kg)</td>
<td>68.34 lbs (31 kg)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td><strong>Environment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC Power Supply</td>
<td>100-240 VAC, 60-50 Hz</td>
<td>100-240 VAC, 60-50 Hz</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Power Consumption (Average/ Maximum)</td>
<td>345 W (full loading)</td>
<td>1390 W / 1668 W</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>1207.5 BTU/h</td>
<td>6824 BTU/h</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>0°C to 40°C (32°F to 104°F) with no direct sunlight on the equipment</td>
<td>10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>–20°C to 70°C (–4°F to 158°F)</td>
<td>–40°C to 65°C (–40°F to 149°F)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Humidity</td>
<td>Storage: 5% to 90% non-condensing</td>
<td>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)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Operating Altitude</td>
<td>Up to 16 404 ft (5000 m)</td>
<td>Up to 7400 ft (2250 m)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>SKU</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Devices</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiNDR-1000F</td>
<td>FNR-1000F</td>
<td>Appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 4× 10GbE SFP+, 2 × 1Gigabit Ethernet connection (management). Netflow order separately.</td>
</tr>
<tr>
<td>FortiNDR-1000F Hardware Bundle</td>
<td>FNR-1000F-BDL-331-DD</td>
<td>FortiNDR-1000F Hardware plus FortiCare Premium, with NDR and ANN engine updates &amp; baseline. FortiNDR-1000F appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 4× 10GbE SFP+, 2× 10Gb GE Copper (supports 10/100/10000 without transceivers), 2× 1 Gigabit Ethernet connection (management). Netflow order separately.</td>
</tr>
<tr>
<td>Netflow for FortiNDR-1000F</td>
<td>FC-10-A11KF-588-02-DD</td>
<td>Netflow Support for FortiNDR-1000F.</td>
</tr>
<tr>
<td>SCADA for FortiNDR-1000F</td>
<td>FC-10-A11KF-723-02-DD</td>
<td>SCADA Support for FortiNDR-1000F.</td>
</tr>
<tr>
<td>FortiNDR-1000F renewal</td>
<td>FC-10-A11KF-331-02-DD</td>
<td>FortiCare Premium with NDR and ANN engine updates and baseline.</td>
</tr>
<tr>
<td>FortiNDR 3500F</td>
<td>FNR-3500F</td>
<td>FortiNDR-3500F appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 4× 10GbE SFP+, 2x 10Gb GE Copper (supports 10/100/10000 without transceivers), 2× 1 Gigabit Ethernet connection (management). Transceivers order separately.</td>
</tr>
<tr>
<td>FortiNDR-3500F Hardware Bundle</td>
<td>FNR-3500F-BDL-331-DD</td>
<td>FortiNDR-3500F bundle - Hardware plus 24×7 FortiCare and NDR and ANN updates and baseline.</td>
</tr>
<tr>
<td>Netflow for FortiNDR-3500F</td>
<td>FC-10-A13K5-588-02-DD</td>
<td>Netflow Support for FortiNDR-3500F.</td>
</tr>
<tr>
<td>SCADA for FortiNDR-3500F</td>
<td>FC-10-A13K5-723-02-DD</td>
<td>SCADA Support for FortiNDR-3500F.</td>
</tr>
<tr>
<td><strong>Virtual Machines</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiNDR-VM16 Subscription License with Bundle</td>
<td>FC3-10-AIVMS-461-02-DD</td>
<td>Subscriptions license for FortiNDR-VM (16 CPU) with 24×7 FortiCare plus NDR and ANN updates and baseline.</td>
</tr>
<tr>
<td>Netflow for VM16</td>
<td>FC3-10-AIVMS-588-02-DD</td>
<td>Netflow Support for FortiNDR-VM16.</td>
</tr>
<tr>
<td>SCADA for VM16</td>
<td>FC3-10-AIVMS-723-02-DD</td>
<td>SCADA Support for FortiNDR-VM16.</td>
</tr>
<tr>
<td>FortiNDR-VM32 Subscription License with Bundle</td>
<td>FC4-10-AIVMS-461-02-DD</td>
<td>Subscriptions license for FortiNDR-VM (32 CPU) with 24×7 FortiCare plus NDR and ANN updates and baseline.</td>
</tr>
<tr>
<td>Netflow for VM32</td>
<td>FC4-10-AIVMS-588-02-DD</td>
<td>Netflow Support for FortiNDR-VM32.</td>
</tr>
<tr>
<td>SCADA for VM32</td>
<td>FC4-10-AIVMS-723-02-DD</td>
<td>SCADA Support for FortiNDR-VM32.</td>
</tr>
<tr>
<td><strong>FortiCare and Updates</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiCare and Updates</td>
<td>FC-10-A13K5-331-02-DD</td>
<td>24×7 FortiCare plus FortiGuard Neural Networks engine updates and baseline.</td>
</tr>
<tr>
<td><strong>Accessories</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.84TB 2.5&quot; SATA SSD with Tray</td>
<td>SP-DFAI-3T</td>
<td>3.84TB 2.5 in. SATA SSD with tray for FortiNDR-3500F.</td>
</tr>
<tr>
<td>10GE SFP+ Transceiver Module, Long Range</td>
<td>FN-TRAN-SFP+LR</td>
<td>10GE SFP+ transceiver module, 10km long range for systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10GE SFP+ Transceiver Module, Short Range</td>
<td>FN-TRAN-SFP+SR</td>
<td>10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10GE copper SFP+ RJ45 Transceiver (30m range) *see pg 5</td>
<td>FN-TRAN-SFP+GC</td>
<td>10GE copper SFP+ RJ45 transceiver module (30m range) for systems with SFP+ slots.</td>
</tr>
<tr>
<td>1GE SFP RJ45 Transceiver Module</td>
<td>FN-TRAN-GC</td>
<td>1GE SFP RJ45 transceiver module for systems with SFP and SFP/SFP+ slots.</td>
</tr>
</tbody>
</table>

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