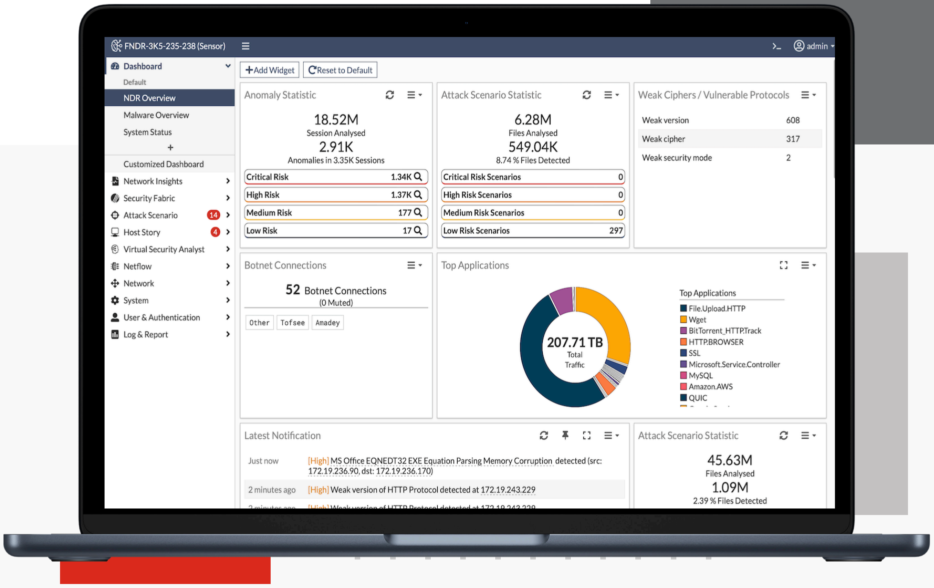
FURTINET

Data Sheet

FortiNDR™ On Premise Solution



Just now [High] MS Office EQNEDT32 EXE Equation Parsing Memory Corruption detected (src: 172.19.236.90, dst: 172.19.236.170)

2 minutes ago [High] Weak version of HTTP Protocol detected at 172.19.243.229

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

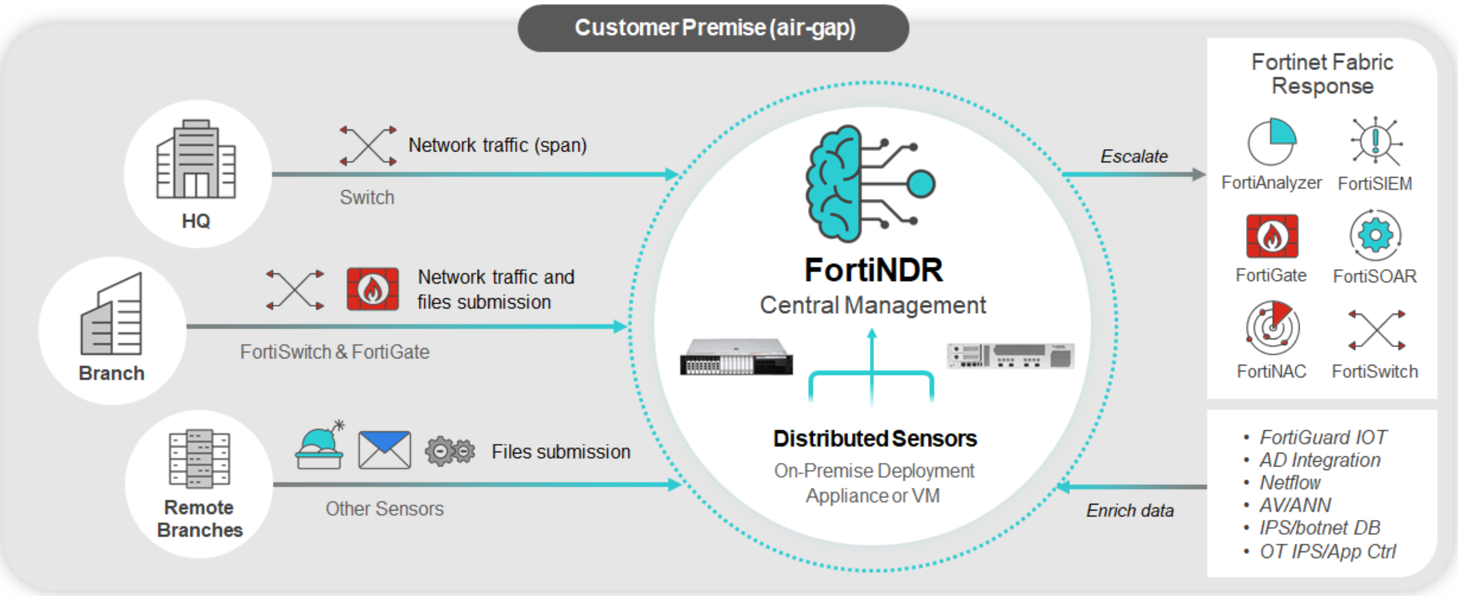
Public Cloud (BYOL)

FortiNDR Key Features

- On Premise solution where no data leaves the customer network
- Integrates 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
- Reduces malware detection and investigation time from minutes to seconds
- Supports OT (Operational Technology) environment with extensive OT attacks detections. Please refer to OT solution brief for details: OT solution brief
- Detects North/South/East/West intrusions accurately
- Detects botnets, weakciphers, as well as Indicator of compromize on network
- Virtual Security Analyst™ to mimic experienced security analyst for outbreak, anomalies, and root causes for malware infections
- Provides 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.

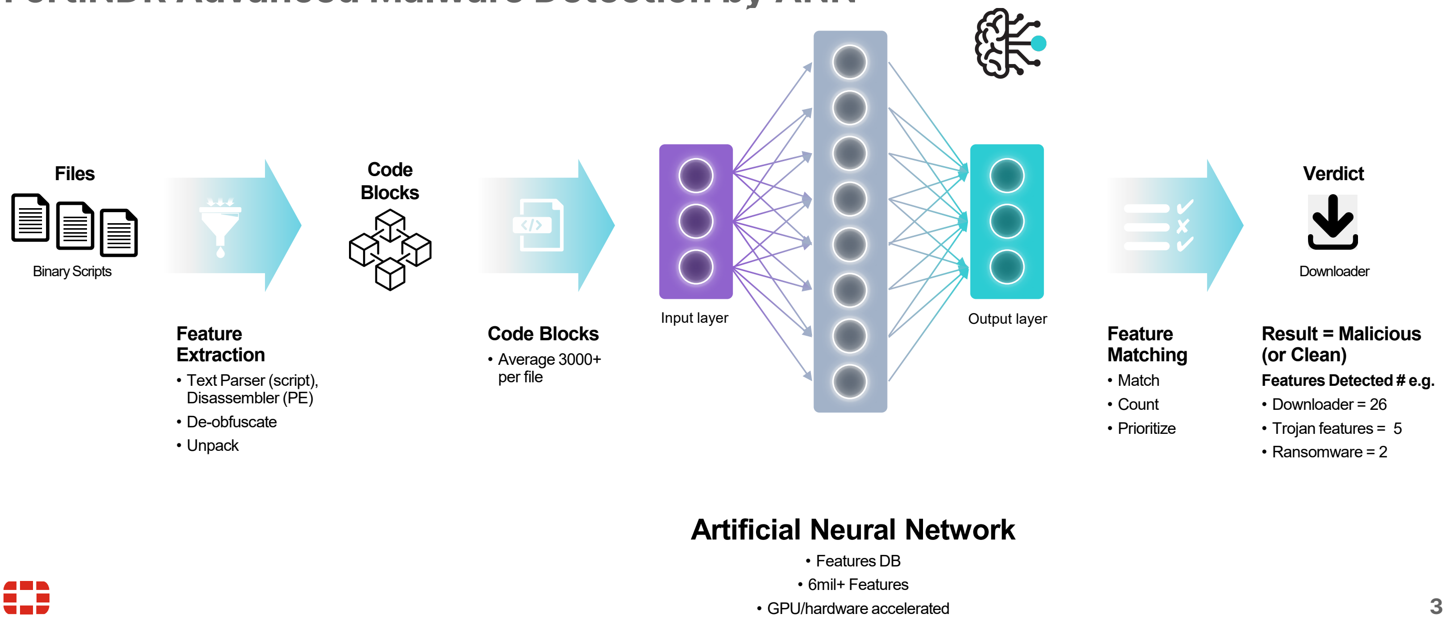
ML-based Traffic Profiling and Malware Detection

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
Sensors, Center, and Standalone Options	Sensor: FortiNDR-1000F, FortiNDR-2500G, VM08, VM16, and VM32 Center: FortiNDR 3600G and FortiNDR VM for Central Management Standalone: FortiNDR-1000F, FortiNDR-2500G, and VM 16, VM32 Public Cloud support (please refer to latest Release Notes for details)
Response Integration	FortiGate, FortiSwitch, FortiNAC quarantine, FortiProxy, 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*

* Please refer to admin guide.

FortiNDR Advanced Malware Detection by ANN



Hardware Specification

Category	FortiNDR 1000F	FortiNDR 2500G	FortiNDR 3600G
Deployment			
Sniffer / SPAN / 802.1q support	✓	✓	—
Deployment Mode	Standalone, Sensor	Standalone, Sensor	Center only
Sensors Managed *	—	—	up to 50
Fortinet Security Fabric Integration (such as FortiGate, FortiSandbox)[1]	✓	✓	—
Hypervisor Support	—	—	—
Netflow Support	✓	✓	—
Hardware Specifications			
Form Factor	2 RU Rackmount	2 RU Rackmount	2 RU Rackmount
Total Interfaces	2× 10/100/1000 RJ45 ports, 4× 10G SFP+, 1x RJ45 console	1x GbE RJ45, 2× 10GbE SFP+, 4× 25GbE SFP28.	1× 1GbE RJ-45 ports 4× 10GbE SFP+ ports
Sniffer/Capture Interfaces[2]	2 (2 x Fiber 10G SFP+)	4× 25GbE SFP28 (can operate in 10Gbps)	—
Transceivers Included	Purchase separately[2]	Purchase separately[2]	Purchase separately[2]
Storage Capacity	2× 7.68 TB (RAID 1) total 7.68 TB (RAID 1)	61.44TB (4× 15.36TB SSDs)	12x hot-swapple HDD (total 176TB)
Default RAID level (RAID software)	1	10	5
Removable Hard Drives	✓	✓	✓
Redundant Hot Swappable Power Supplies	✓	✓	✓
Custom GPUs for ANN Acceleration	—	—	✓
System Performance			
NDR Sniffer Throughput			
HTTP	single 10/ dual ports 20 Gbps	34 Gbps (4 ports)	—
Enterprise Mix (single/dual port)	single 10/ dual ports 20 Gbps	34 Gbps (4 ports)	—
Netflows (flows/second)	100k	200k	—
Malware Analysis Throughput (files per hour)[3]	170k	252k	—
Malware Classification	26	26	26
Dimensions			
Height x Width x Length (mm)	88.9 × 444.5 × 574.04	88 × 438 × 695.8 (w/o handle), 88 × 483 × 740.8 (w/ handle)	88 × 438 × 750
Weight	34.6 lbs (16 kg)	40 lbs (18.14kg)	75.12 lbs (34 kg)
Environment			
AC Power Supply	100-240 VAC, 60-50 Hz	100-240 VAC, 60-50 Hz	200-240 VAC, 60-50 Hz
Power Consumption (Average/ Maximum)	163 W (idle) / 345 W (full loading)	524.8W (idle) / 682.2W (full loading)	1046 W / 1359 W
Heat Dissipation	1207.5 BTU/h	2327.8 BTU/h	4637 BTU/h
Operating Temperature	0°C to 40°C (32°F to 104°F) with no direct sunlight on the equipment	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)
Storage Temperature	−20°C to 70°C (−4°F to 158°F)	−20°C to 70°C (−4°F to 158°F)	−20°C to 70°C (−4°F to 158°F)
Humidity	Storage: 5% to 90% non-condensing	5% to 90%	5% to 90% non-condensing
Operating Altitude	Up to 16 404 ft (5000 m)	10 000 ft (3048 m)	10 000 ft (3048 m)
Compliance			
Certifications	FCC Part 15 Class A, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, ISED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB	FCC, ISED, RCM, VCCI, CE, BSMI, UL/cUL, CB

* For deployment more than 20 please consult Fortinet system engineers for details.

Please click here for hardware quick start guide.

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

[2] If copper on FNR-1000F or FNR-3600G is required (e.g. for mgmt or sniffer), customer can use 1G with Fortinet FN-TRAN-GC.
If 10G copper is reqiured on FNR-1000F or FNR-3600G, 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 NDR-1000F and NDR-3600G platforms.
FN-TRAN-SFP28-LR and FN-TRAN-SFP28-SR can be used on FNR-2500G on 4× 25GB ports.

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

Virtual Machine Specification

Category	FortiNDR VM08	FortiNDR VM 16	FortiNDR VM 32	FortiNDR VM Central Management
Deployment				
Sniffer / SPAN / 802.1q support	✓	✓	✓	—
Deployment Mode	Sensor only (requires center purchase)	Standalone, Sensor (center optional)	Standalone, Sensor (center optional)	Center (requires sensors purchase)
Sensors Managed *	—	—	—	Up to 20
Fortinet Security Fabric Integration (such as FortiGate, FortiSandbox)[1]	✓	✓	✓	—
Hypervisor Support	ESXi 6.7 U2+, KVM	ESXi 6.7 U2+, KVM	ESXi 6.7 U2+, KVM	KVM, ESXi 6.7 U2+
Netflow Support	Not supported	Required	Required	Yes
Hardware Specifications				
Form Factor	—	—	—	
Total Interfaces	5x virtual interfaces	5x virtual interfaces	5x virtual interfaces	5x virtual Interfaces
Sniffer/Capture Interfaces[2]	2 x vNIC	2 x vNIC	2 x vNIC	—
Transceivers Included	—	—	—	—
Storage Capacity	1-8TB	1-8TB	1-8TB	1-20TB
Default RAID level (RAID software)	Hypervisor dependent	Hypervisor dependent	Hypervisor dependent	Hypervisor dependent
Technical Specifications				
vCPU Support (Minimum / Recommended)	8/8	16/16	32/32	48/64
Memory Support (Minimum / Recommended)	64 GB (minimum)	128 GB (minimum)	256 GB (minimum)	384 GB / 512 GB
Recommended Storage	1 TB to 8 TB	1 TB to 8 TB	1 TB to 8 TB	15 TB / 20 TB
System Performance				
NDR Sniffer Throughput**				
HTTP (single port only)	750 Mbps	6 Gbps	10 Gbps	—
Enterprise Mix (single port only)	500 Mbps	4 Gbps	10 Gbps	—
Netflows (flows/second)	Not supported	35k	200k	—
Malware Analysis Throughput (files per hour)[3]	10k (AV only)	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.

Ordering Information

PRODUCT	SKU	DESCRIPTION
Devices*		
FortiNDR-1000F	FNR-1000F	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.
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. 4× 10GbE SFP+, 2× 10Gb GE Copper (supports 10/1000/10000 without transceivers), 2× 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	OT Security Service for FortiNDR-1000F (OT IPS and application control, ML anomalies detection and OT malware detections).
FortiNDR-1000F renewal	FC-10-AI1KF-331-02-DD	FortiCare Premium with NDR and ANN engine updates and baseline.
FortiCare and Updates	FC-10-AI3K5-331-02-DD	24×7 FortiCare plus FortiGuard Neural Networks engine updates and baseline.
FortiNDR 2500G	FNR-2500G	Appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. Support Standalone and Sensor mode. 1x GbE RJ45, 2× 10GbE SFP+, 4× 25GbE SFP28. Sensor and standalone mode only. Netflow and OT Security Service order separately. Transceivers and breakout cables purchased seperately, see datasheet for details.
	FNR-2500G-BDL-331-DD	FortiNDR-2500G Hardware plus FortiCare Premium, with NDR and ANN engine updates & baseline. Support Standalone and Sensor mode. 1x GbE RJ45, 2× 10GbE SFP+ (supports 10/1000/10000 without transceivers), 2× 1 Gigabit Ethernet connection (management). Netflow & OT Security Service order separately. Transceivers purchased seperately, see datasheet for details.
	FC-10-AI25G-331-02-DD	FortiCare Premium with NDR and ANN engine updates and baseline
	FC-10-AI25G-588-02-DD	Netflow Support for FortiNDR-2500G
	FC-10-AI25G-723-02-DD	OT Security Service for FortiNDR-2500G (OT IPS and application control, ML anomalies detection and OT malware detections)
FortiNDR 3600G	FNR-3600G	Appliance for Network Anomalies and zero-day/Malware Detection. Center mode only (Please purchase physical or virtual sensors). 12x hot-swappable HDD (fully populated). 1x RJ45 console port. 1× 1GbE RJ45 ports. 4× 10GbE SFP+ ports. 1+1 redundant power input.
	FNR-3600G-BDL-1024-DD*	FortiNDR-3600G Hardware plus FortiCare Premium, with NDR and OT Security Services Updates. Center mode only (Please purchase physical or virtual sensors). 12x hot-swappable HDD (fully populated). 1x RJ45 console port. 1× 1GbE RJ-45 ports. 4× 10GbE SFP+ ports. 1+1 redundant power input.
Virtual Machines		
FortiNDR VM08 Subscription License with Bundle	FC2-10-AIVMS-461-02-DD	Subscriptions license for FortiNDR-VM (8 CPU) with Forticare Premium with NDR and ANN engine updates and baseline. No netflow support and SCADA license purchased separately.
	FC2-10-AIVMS-723-02-DD	OT Security Service for FortiNDR-VM08 (OT IPS and application control, ML anomalies detection and OT malware detections).
FortiNDR-VM16 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.
Netflow for VM16	FC3-10-AIVMS-588-02-DD	Netflow Support for FortiNDR-VM16.
SCADA for VM16	FC3-10-AIVMS-723-02-DD	OT Security Service for FortiNDR-VM16 (OT IPS and application control, ML anomalies detection and OT malware detections).
FortiNDR-VM32 Subscription License with Bundle	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 VM32	FC4-10-AIVMS-588-02-DD	Netflow Support for FortiNDR-VM32.
SCADA for VM32	FC4-10-AIVMS-723-02-DD	OT Security Service for FortiNDR-VM32 (OT IPS and application control, ML anomalies detection and OT malware detections).
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		
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)	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.

* Premium RMA is available, please refer to Price List for details.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

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

August 1, 2025