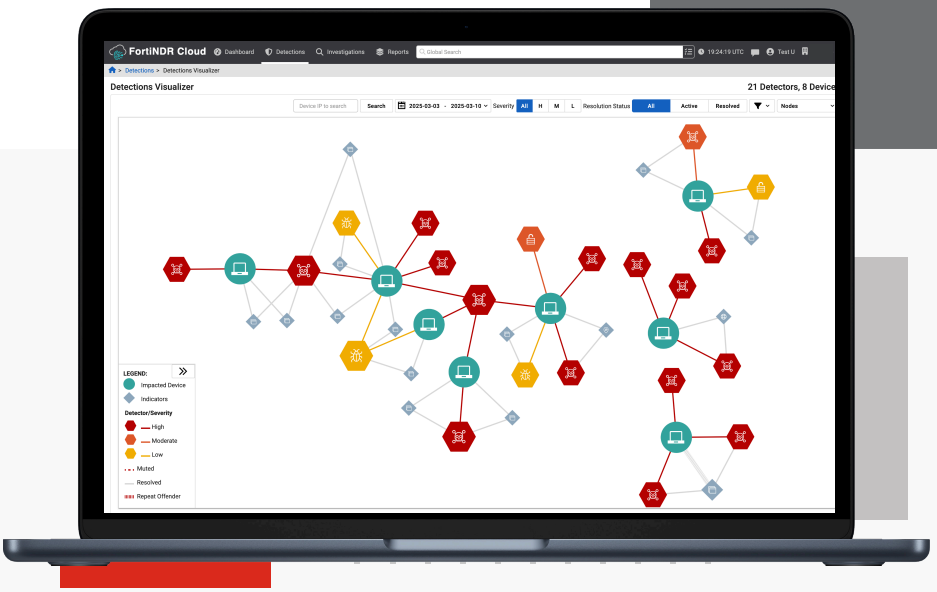
FortiNDR™ Cloud



Highlights

- 365-day historical deep network traffic visibility and analytics
- Curated threat intelligence, powered by FortiGuard Labs, for reduced false positives
- Fortinet Security Fabric and third-party integrations
- Leverage AI, expert analysis, and cloud compute for threat detection
- Coverage for over 90% of MITRE ATT&CK techniques

Network Detection and Response

Fortinet's SaaS-based FortiNDR Cloud leverages artificial intelligence (AI) and machine learning (ML), behavioral, and human analysis to inspect network traffic to detect malicious behavior early while reducing false positives. FortiNDR Cloud provides unified network traffic visibility across multi-cloud and hybrid environments as well as distributed workforces and constrained, mission-critical environments.

FortiNDR Cloud automatically identifies anomalous and malicious behavior, provides risk scores, and shares relevant threat intelligence to assist security teams in prioritizing response efforts.

As the world's only Guided-SaaS NDR, FortiNDR Cloud provides dedicated Technical Success Manager (TSM) support. TSMs act as trusted advisors who share findings, tune configurations, and help organizations optimize NDR deployments.

Highlights

Key Features

- Guided SaaS with trusted advisors
- 365-day data retention for retrospective analysis and threat hunting
- Hunt adversaries with Guided Queries
- Automatic and manual response for quarantine and control
- Orchestrated response with integrations with Fortinet and third party tools including CrowdStrike, FortiEDR, Splunk, Cortex, FortiSIEM, FortiSOAR, and Microsoft Sentinel
- Global crowdsourced threat intelligence from numerous third-party feeds and proprietary sensors

Basic Competencies

Improved Visibility of Threats

Real-time, automated investigation of network security incidents and extended historical network visibility enable a faster, more comprehensive response to threats. Because the impact of an intrusion increases over time, real-time response is the best way to minimize damage.

Get Expertise on Demand

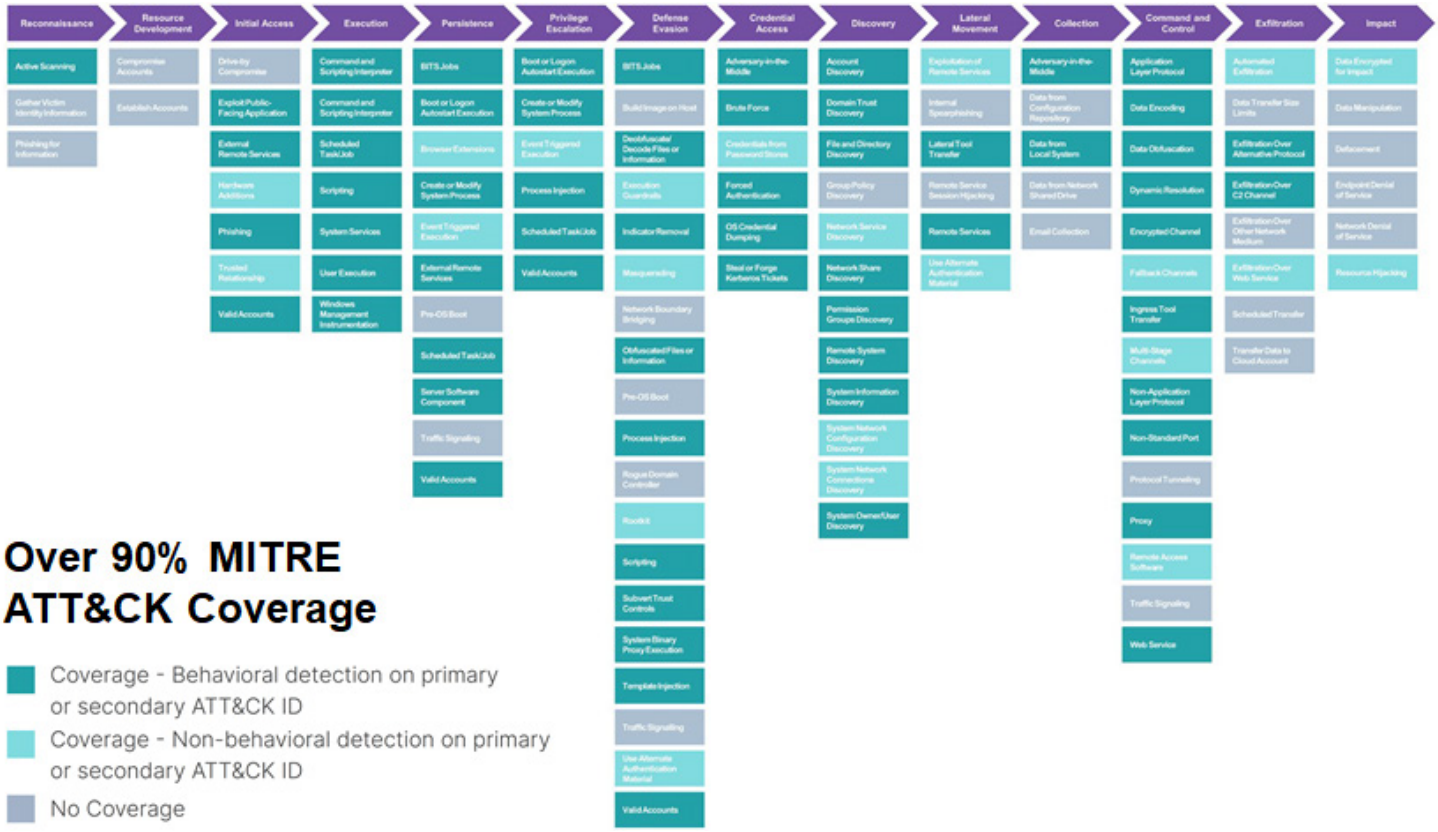
FortiNDR Cloud helps security teams overcome the skills gap challenge by providing Technical Success Manager (TSM) support. TSMs act as trusted advisors who share findings, tune configurations, and help organizations optimize NDR deployments.

Fewer Distractions from False Positives and Detection Tuning

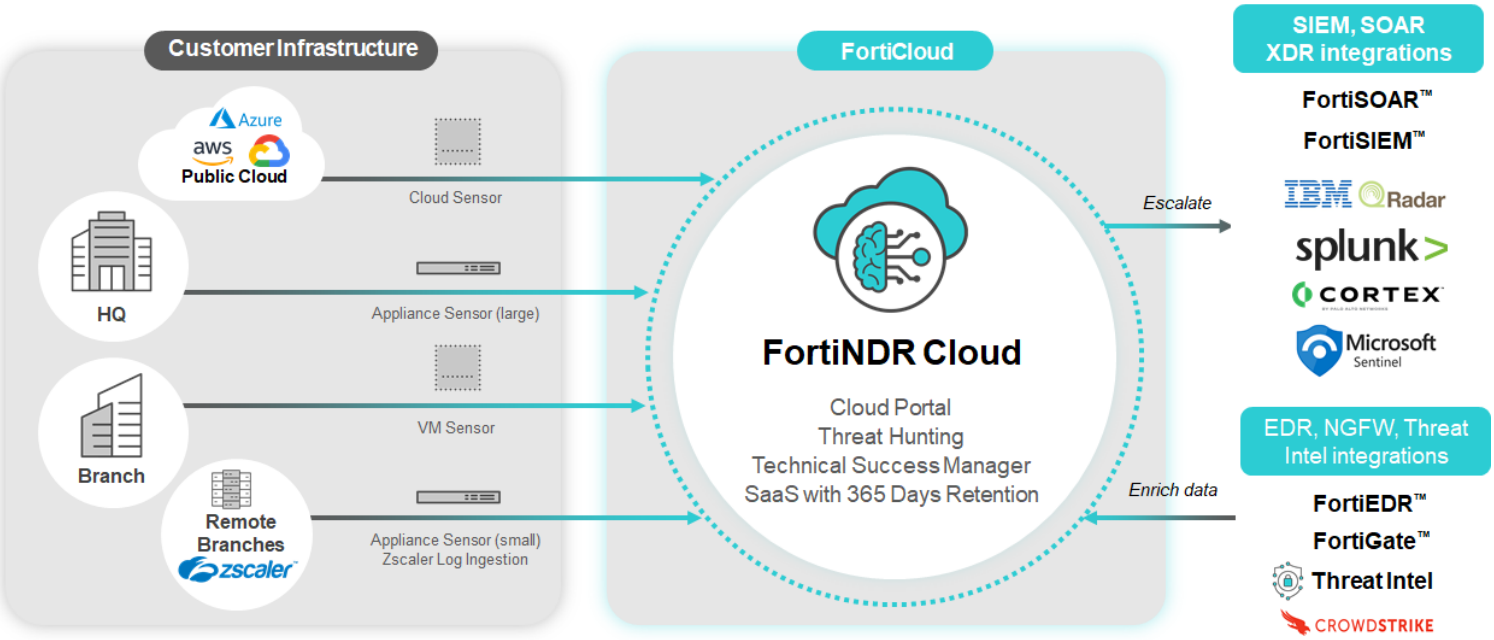
With threat analysis and detection tuning provided in real-time, organizations are less vulnerable while awaiting a vendor's application patch or anti-malware signature.

365-day Data Retention for Retrospective Analysis and Threat Hunting

FortiNDR Cloud retains rich network metadata for 365 days, enabling a comprehensive investigation. This data ensures newly discovered tools, tactics, and procedures can be retroactively investigated to discover if and when threats may have infiltrated the customer's network.



FortiNDR™ Cloud Deployment



Features	FortiNDR Cloud
Deployment	SaaS
Security Analyst	Guided-SaaS with TSM* (Technical Success Manager)
Data Storage Location	Cloud-based (US or EU)
Data Retention	365 Days
Investigation / Threat Hunting	Guided Queries and Parallel Hunting
Malware Identification	FortiGuard Malware feed; VirusTotal lookup
MITRE ATT&CK Framework Mapping	Detections and Playbooks mapped to MITRE ATT&CK Framework
Response Integration	Fortinet Security Fabric Third-party API (Rest) MetaStream (AWS S3) Integrations include CrowdStrike Falcon EDR, FortiEDR, FortiSIEM, FortiSOAR, Cortex, Splunk, QRadar, Microsoft Sentinel, FortiGate, and Crowdstrike SIEM
Sensors	Hardware: FortiNDR Cloud-2540G (Extra Large sensor) Hardware:FortiNDR Cloud-900G (Large sensor) Hardware: FortiNDR Cloud-500G (Small sensor) Virtual Sensors (AWS / Azure / ESXi / HyperV / GCP / KVM)
FortiGuard Labs Threat Research	✓

* for customers over 1Gbps

FortiNDR Cloud Sensor Specifications

Category	FNDR Cloud 500G small sensor	FNDR Cloud 900G large sensor	FNDR Cloud 2540G extra large sensor	FNDR Cloud Virtual Sensors
Deployment				
Sniffer / SPAN / 802.1q support	✓	✓	✓	✓
Cloud based sensors + SaaS portal	✓	✓	✓	✓
Hypervisor Support	—	—	—	ESXi6.7 U2+, KVM, HyperV, GCP, AWS, Azure
Hardware Specifications				
Total Interfaces	2× 10/25GbE SFP28 4× 1GbE RJ45 2× 10GbE RJ45	2× 10/25GbE SFP28 4× 1GbE RJ45 2× 10GbE RJ45	1× 1GbE RJ45 (mgmt), 2× 10GbE SFP+, 2× 25GbE SFP28, 1x Console (RJ45)	1 mgmt + min 1 TAP
Sniffer Interfaces	3 × 1Gbps (1Gbps Ethernet RJ45) 2 × 10Gbps (10Gbps Ethernet RJ45) 2 × 10/25GbE SFP28 (supports SFP+ SR/LR for 10Gbps and SFP28 SR transceivers for 25Gbps)	3 × 1Gbps (1Gbps Ethernet RJ45) 2 × 10Gbps (10Gbps Ethernet RJ45) 2 × 10/25GbE SFP28 (supports SFP+ SR/LR for 10Gbps and SFP28 SR transceivers for 25Gbps)	2× 10GbE SFP+ 2× 25GbE SFP28 (breakout cable supported)	min 1 x vNIC max 3 x vNIC
Transceivers Included	purchase separately	purchase separately	purchase separately	—
Storage Capacity	2 × 1.6TB	2 × 1.6TB	3.84TB (4× 960GB 2.5" NVMe SSD)	100 (min) - 300 GB (recommended)
Default RAID level (RAID software)	RAID 1	RAID 1	10	Hypervisor dependent
Removable Hard Drives	Yes	Yes	Yes	—
Redundant Hot Swappable Power Supplies	Yes	Yes	Yes	—
Technical Specifications				
vCPU Support (Recommended)	—	—	—	16
Memory Support (Minimum / Recommended)	—	—	—	16 GB / 32 GB
System Performance				
NDR Sniffer Throughput* (metadata processing across all ports)	14Gbps (enterprise mix)	18Gbps (enterprise mix)	38 Gbps (enterprise mix)	Hypervisor dependent
Malware Lookups	Hash lookup (Virus Total) and FortiGuard Malware Feed	Hash lookup (Virus Total) and FortiGuard Malware Feed	Hash lookup (Virus Total) and FortiGuard Malware Feed	Hash lookup (Virus Total) and FortiGuard Malware Feed
Dimensions				
Height x Width x Length (mm)	42.8 × 482 × 809.04	42.8 × 482 × 809.04	88 × 483 × 740.8 mm with handle 88 × 438 × 695.8 mm w/o handle	—
Weight	17.23 kg / 38 lbs	17.23 kg / 38 lbs	18.14 kg	—
Environment				
AC Power Supply	100-240 VAC, 50/60 Hz, 12-6.3A	100-240 VAC, 50/60 Hz, 12-6.3A	100-240 VAC, 60-50 Hz	—
Power Consumption (Average/ Maximum)	350 W / 500 W	455 W / 685 W	524.8 W / 682.2 W	—
Heat Dissipation	1706 (BTU/h)	2337.3 (BTU/h)	2327.8 BTU/h	—
Operating Temperature	10°C to 35°C (50°F to 95°F)	10°C to 35°C (50°F to 95°F)	0°C to 40°C (32°F to 104°F) with no direct sunlight on the equipment	—
Storage Temperature	-40 to 65°C (-40 to 149°F)	-40 to 65°C (-40 to 149°F)	–20°C to 70°C (–4°F to 158°F)	—
Humidity	Op: 8%RH with -12°C minimum dew point to 80%RH with 21°C (69.8°F) maximum dew point; Non-Op: 5% to 95%RH with 27°C (80.6°F) maximum dew point.	Op: 8%RH with -12°C minimum dew point to 80%RH with 21°C (69.8°F) maximum dew point; Non-Op: 5% to 95%RH with 27°C (80.6°F) maximum dew point	5% to 90% 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	10000ft / 3048m	10000ft / 3048m	Up to 10 000 ft (3048 m)	—
Compliance				
Certifications	FCC, ISED, CE, RCM, VCCI, BSMI (Class A), 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	—

*Using FortiTester default Enterprise Profile

Ordering Information

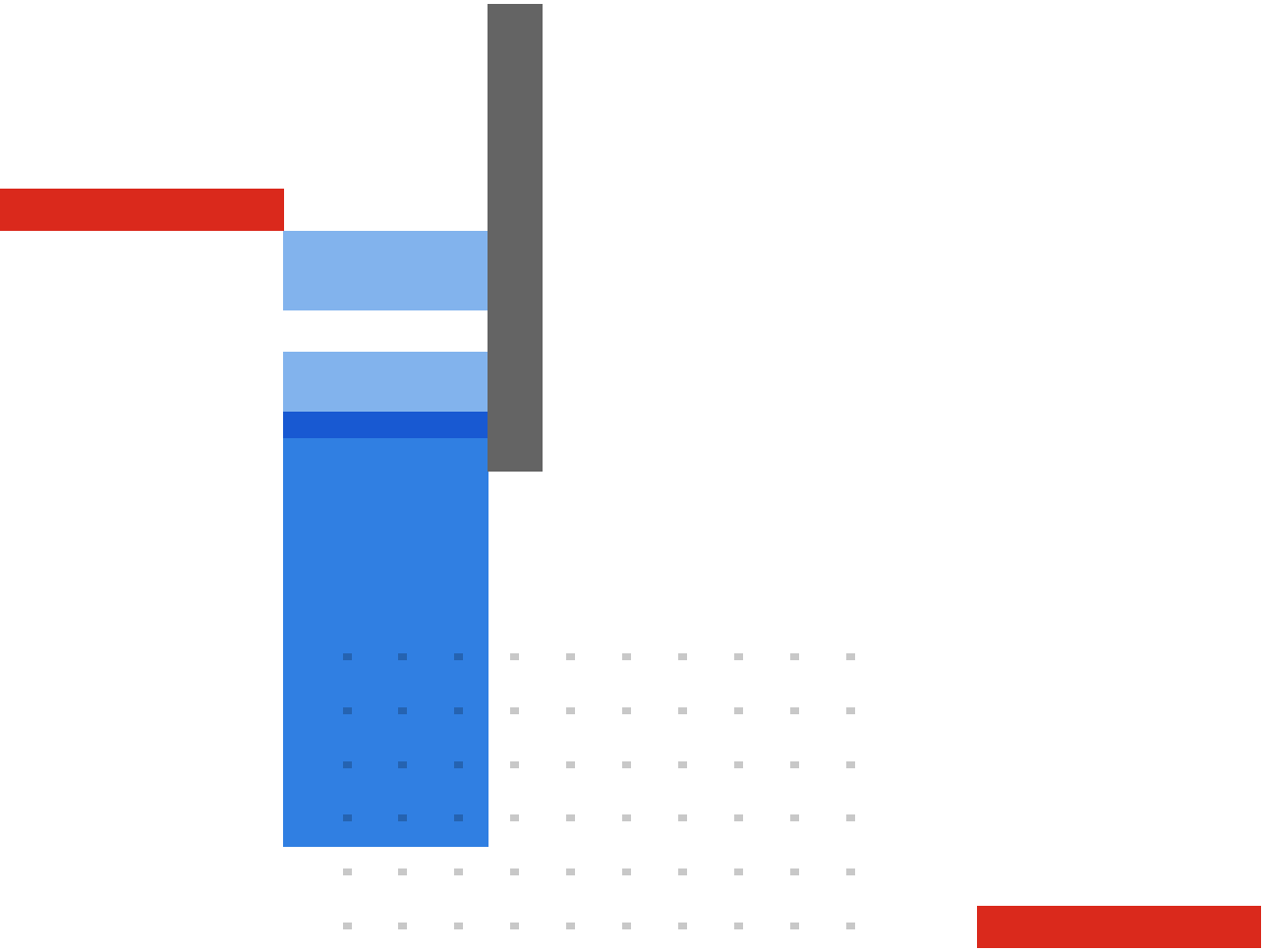
FORTINDR CLOUD		
Product	**SKU**	**Description**
FortiNDRCloud-SAAS Services	FC1-10-NDRCL-1244-02-DD	Annual Subscription license for FortiNDR Cloud Guided-SaaS Platform with Detections, Investigations, Playbooks, and Reports at 100Mbps of metered usage (Stackable). Includes FortiCare premium. Includes unlimited VM sensors. Physical Sensors purchased separately.
True Up Usage	NDRC-TRUE-UP-1MTH100M	Throughput True-up SKU for traffic overages in FortiNDR Cloud for 100Mbps of metered usage.
FortiNDRCloud-500G	FNRC-500G	FortiNDRCloud 500G (small) physical sensor to deliver data to FortiNDR Cloud SaaS Platform. Hardware Only. 1U with 2× 10/25GbE SFP28, 4× 1GbE RJ45, and 2× 10GbE RJ45. Must purchase support.
Small Sensor (500G) Licence and Suppport	FC-10-NDR5G-247-02-DD	Annual license for support for FNRC-500G (small) sensor and forwarding traffic to the FortiNDR Cloud SaaS Platform, includes FortiCare premium.
FortiNDRCloud-900G	FNRC-900G	FortiNDRCloud 900G (large) physical sensor to deliver data to FortiNDR Cloud SaaS Platform. Hardware Only. 1U with 2× 10/25GbE SFP28, 4× 1GbE RJ45, and 2× 10GbE RJ45. Must purchase support.
Large Sensor (900G) Licence and Suppport	FC-10-NDR9G-247-02-DD	Annual license for support for FNRC-900G (large) sensor and forwarding traffic to the FortiNDR Cloud SaaS Platform, includes FortiCare premium.
FortiNDR Cloud-2540G	FNRC-2540G	FortiNDR Cloud 2540G (extra large) physical sensor to deliver data to FortiNDR Cloud SaaS Platform. Hardware Only. 2U with 1x GbE copper, 2× 10GbE SFP+, 2× 25GbE SFP28. Must purchase support. Transceivers *not* included.
Extra Large Sensor (2540G) Licence and Suppport	FC-10-ND25G-247-02-DD	FortiNDRCloud-2540G Annual license for support for FNRC-2540G (extra-large) sensor and forwarding traffic to the FortiNDR Cloud SaaS Platform, includes FortiCare premium.
FortiNDR Cloud Log Ingestion	FC1-10-NDRCL-1247-02-DD	Annual Subscription license for FortiNDR Cloud to intake 3rd party logs for detections (e.g. Zscaler). SKU is based on 100 ESP (events per second). Stackable. Must purchase FortiNDR Cloud Guide SaaS with this subscription.
Accessories		
10GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range 10km, LC connector, SMF, 1310nm, 0°C to 85°C, for systems with SFP+ slots.
10GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots.
25GE SFP28 Transceiver Module, Short Range	FN-TRAN-SFP28-SR	25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots.
***40G/100G QSFP+ to 4x SFP+/SFP28 Optical Breakout 1m**	FG-TRAN-QSFP-4XSFP	40G/100G QSFP+/QSFP28 to SFP+/SFP28 parallel breakout MPO to 4xLC connectors, OM3 MMF, 1m, transceivers not included.
***40G/100G QSFP+ to 4x SFP+/SFP28 Optical Breakout 5m**	FG-TRAN-QSFP-4SFP-5	40G/100G QSFP+/QSFP28 to SFP+/SFP28 parallel breakout MPO to 4xLC connectors, OM3 MMF, 5m, transceivers not included.

* For monitoring 40 Gbps ports on switch, use breakout cable on 2540G to breakout into 4 × 10 Gbps

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.



FORTINET

www.fortinet.com

August 7, 2025

FNDR-CL-DAT-R06-20250807