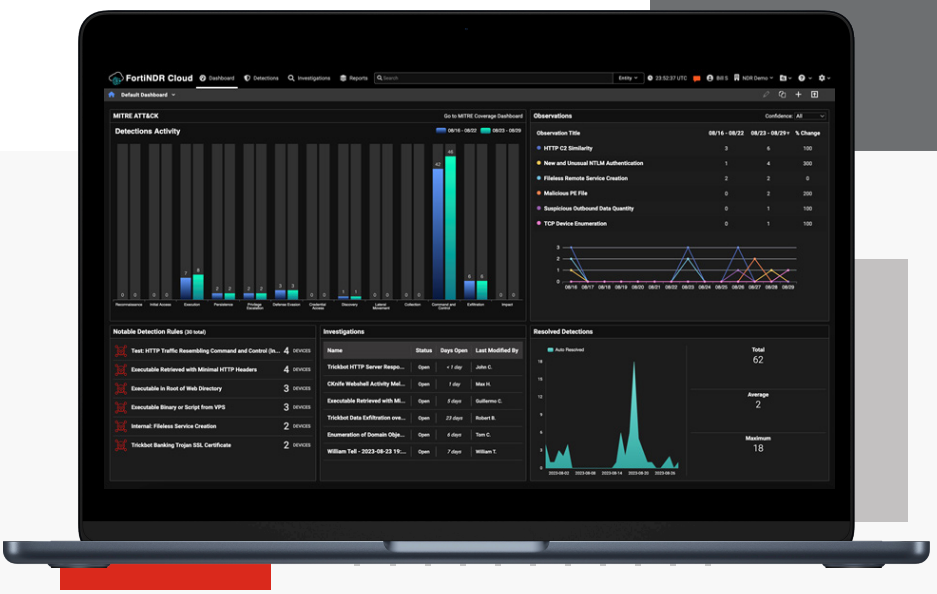
FortiNDR™ Cloud



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

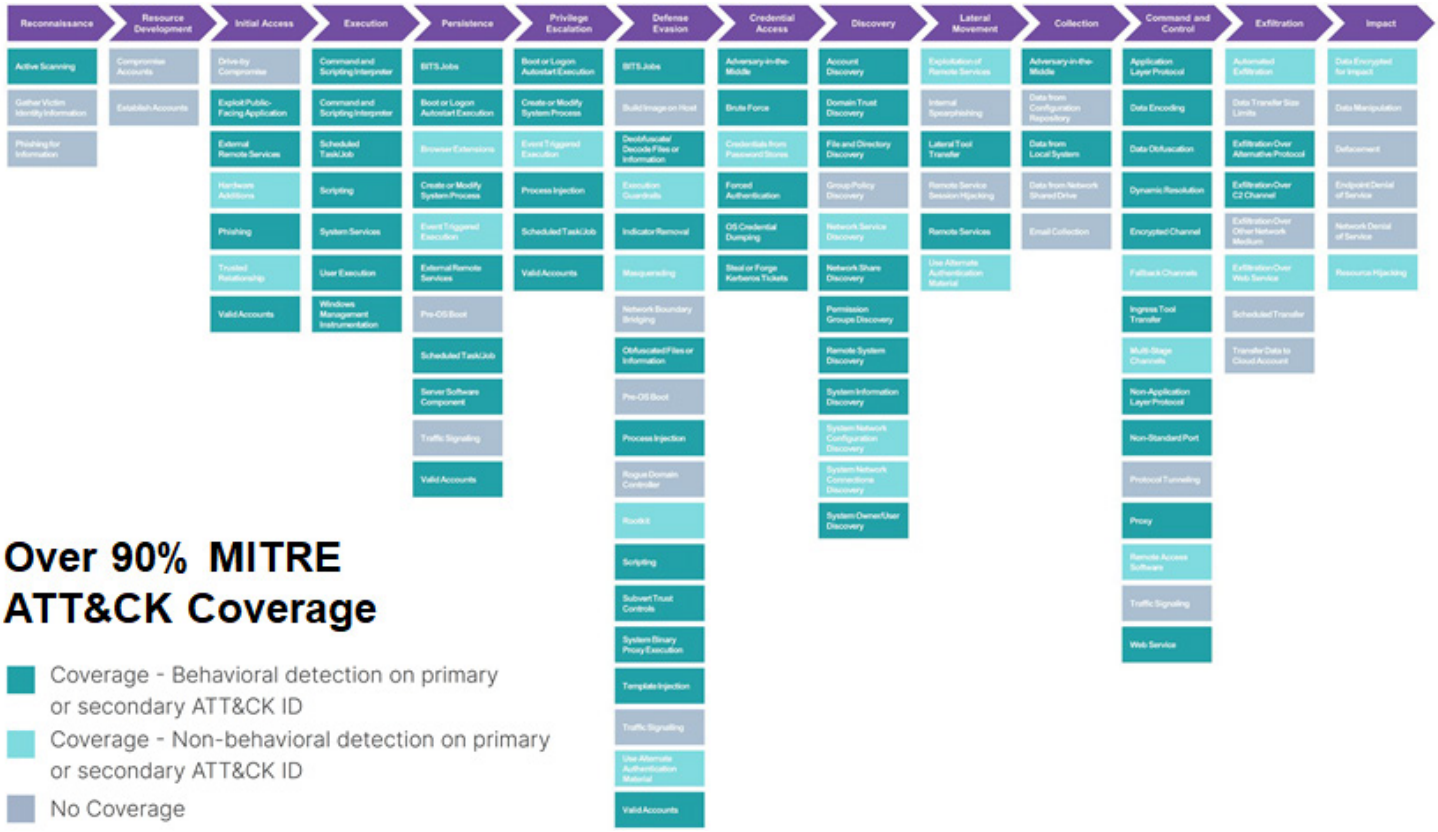
FortiNDR Cloud helps security teams overcome the skills gap challenge by providing Technical Success Manager (TSM) support. TSMs act as trusted advisors who share findings, tune configurations, and help organizations optimize NDR deployments.

Fewer Distractions from False Positives and Detection Tuning

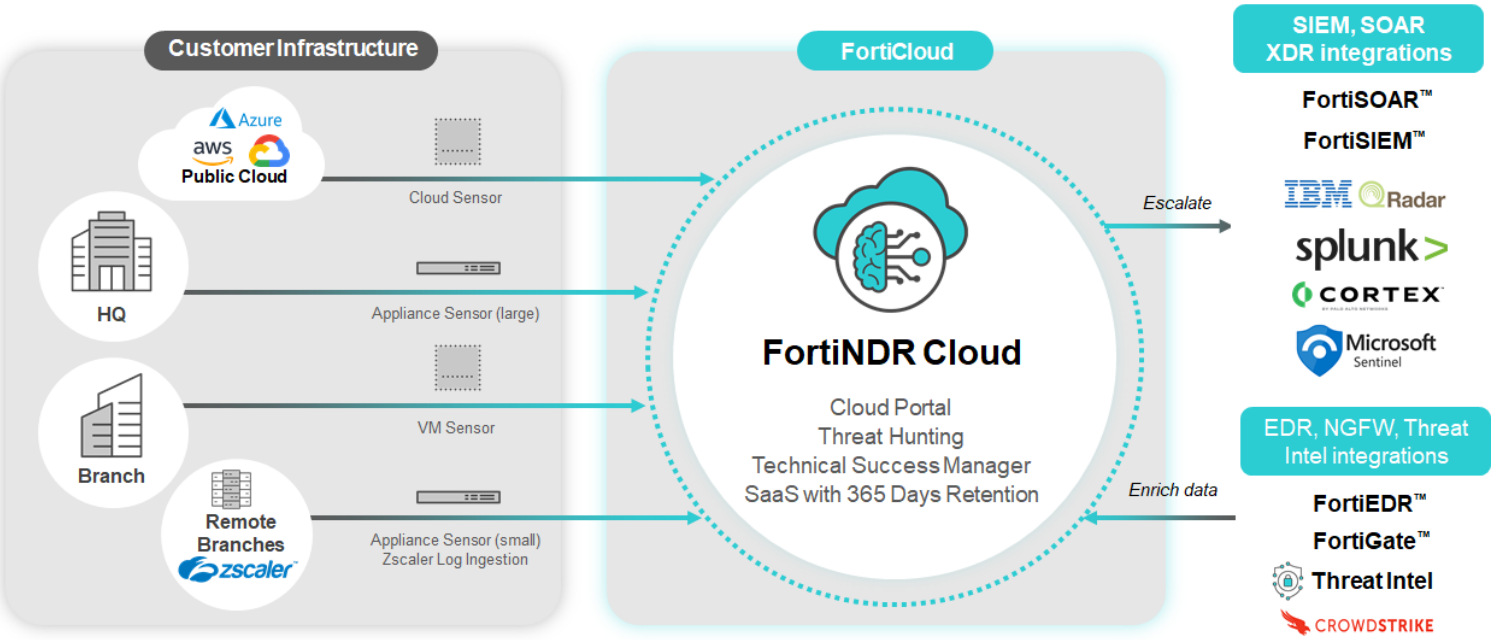
With threat analysis and detection tuning provided in real-time, organizations are less vulnerable while awaiting a vendor's application patch or anti-malware signature.

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 with CrowdStrike, FortiEDR, FortiSIEM, FortiSOAR, Cortex, Splunk, QRadar, and Microsoft Sentinel
Sensors	Hardware:FortiNDR Cloud-900F (Large sensor) Hardware: FortiNDR Cloud-500F (Small sensor) Virtual Sensors (AWS / Azure / ESXi / KVM / GCP)
FortiGuard Labs Threat Research	✓

FortiNDR Cloud Sensor Specifications

Category	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	✓	✓	✓
Hypervisor Support	—	—	ESXi6.7 U2+, KVM
Hardware Specifications			
Total Interfaces	1 × 1G Copper, 2 × 10G SFP+, 2 × 10G Copper	1 × 1G Copper, 2 × 10G SFP+, 2 × 10G Copper	1 mgmt + min 1 TAP
Sniffer Interfaces	5 (1 × 1G Copper, 2 × 10G SFP+, 2 × 10G Copper)	5 (1 × 1G Copper, 2 × 10G SFP+, 2 × 10G Copper)	min 1 x vNIC max 3 x vNIC
Transceivers Included	2× 10G multimode	4× 10G multimode	—
Storage Capacity	890 GB	890 GB	100 (min) - 300 GB (recommended)
Default RAID level (RAID software)	10	10	Hypervisor dependent
Removable Hard Drives	Yes	Yes	—
Redundant Hot Swappable Power Supplies	Yes	Yes	—
Technical Specifications			
vCPU Support (Recommended)	—	—	16
Memory Support (Minimum / Recommended)	—	—	16 GB / 32 GB
System Performance			
NDR Sniffer Throughput	2 Gbps (metadata processing) across all ports	10 Gbps (metadata processing) across all ports	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
Dimensions			
Height x Width x Length (mm)	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	25.9 kg	25.9 kg	—
Environment			
AC Power Supply	100-240 VAC, 60-50 Hz	100-240 VAC, 60-50 Hz	—
Power Consumption (Average/ Maximum)	276 W / 390 W	409 W / 619 W	—
Heat Dissipation	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	—
Storage Temperature	–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. 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 10 000 ft (3048 m)	Up to 10 000 ft (3048 m)	—
Compliance			
Safety Certifications	FCC, ISED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB	FCC, ISED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB	—

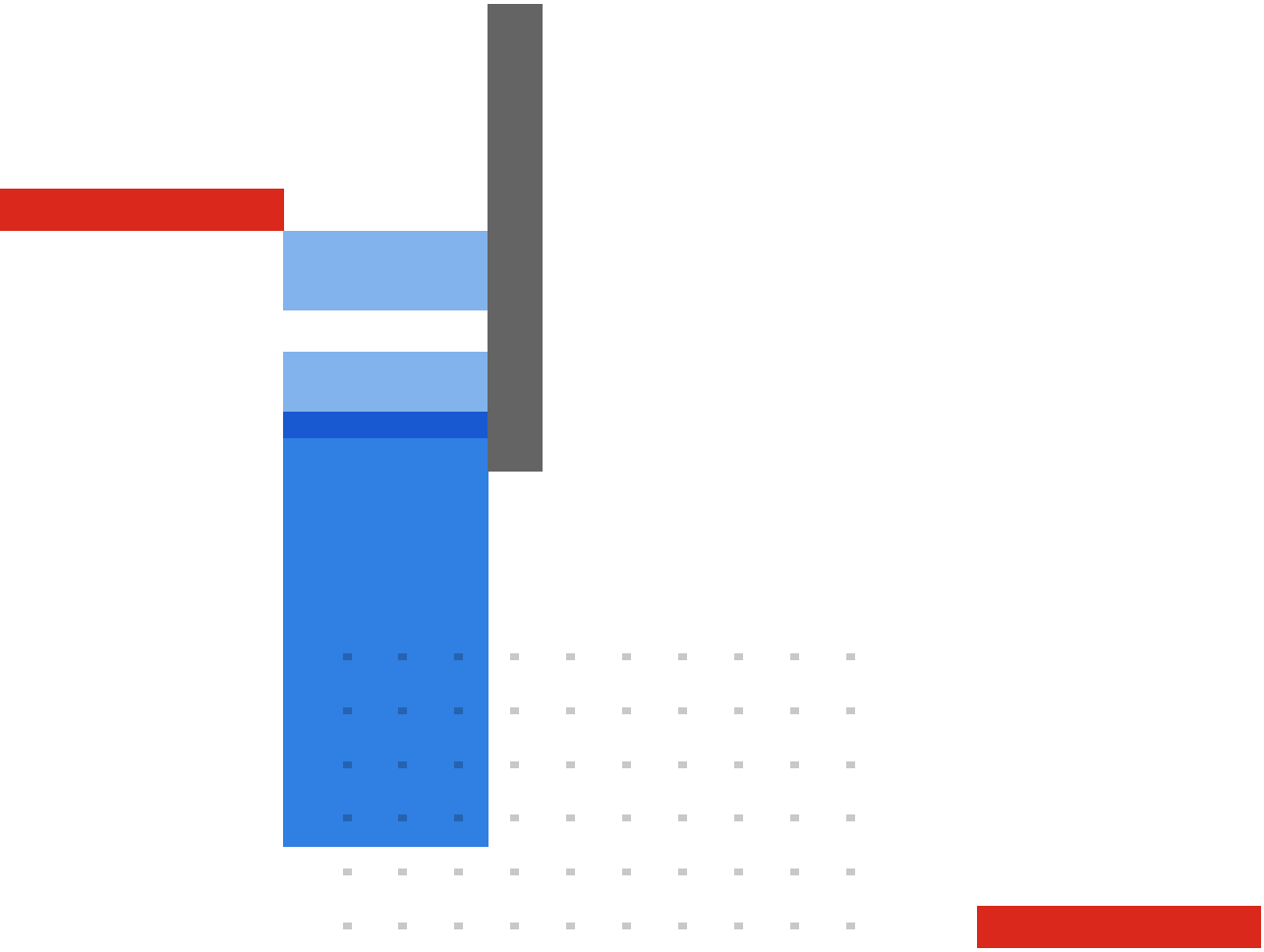
Ordering Information

FORTINDR 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 2x Copper / 2x 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 2x Copper / 2x Fiber SFP+. Must purchase support. Ship with 4× 10G multimode transceivers.
Large Sensor (900F) 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.
FortiNDR Cloud log Ingestion	FC1-10-NDRCL-1009-02-DD	Annual Subscription license for FortiNDR Cloud to consume third party logs for detections (for example, Zscaler). SKU is based on 1000 EPS (events per second). Must purchase FortiNDR Cloud Guide SaaS with this subscription.

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

November 21, 2024

FNDR-CL-DAT-R03-20241121