ORDERING GUIDE

FortiNDR

FortiNDR Cloud and FortiNDR On-premise represent 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 datacenters, to identify threats, especially those which may be already persistent in the network.

Two different NDR deployments are available:

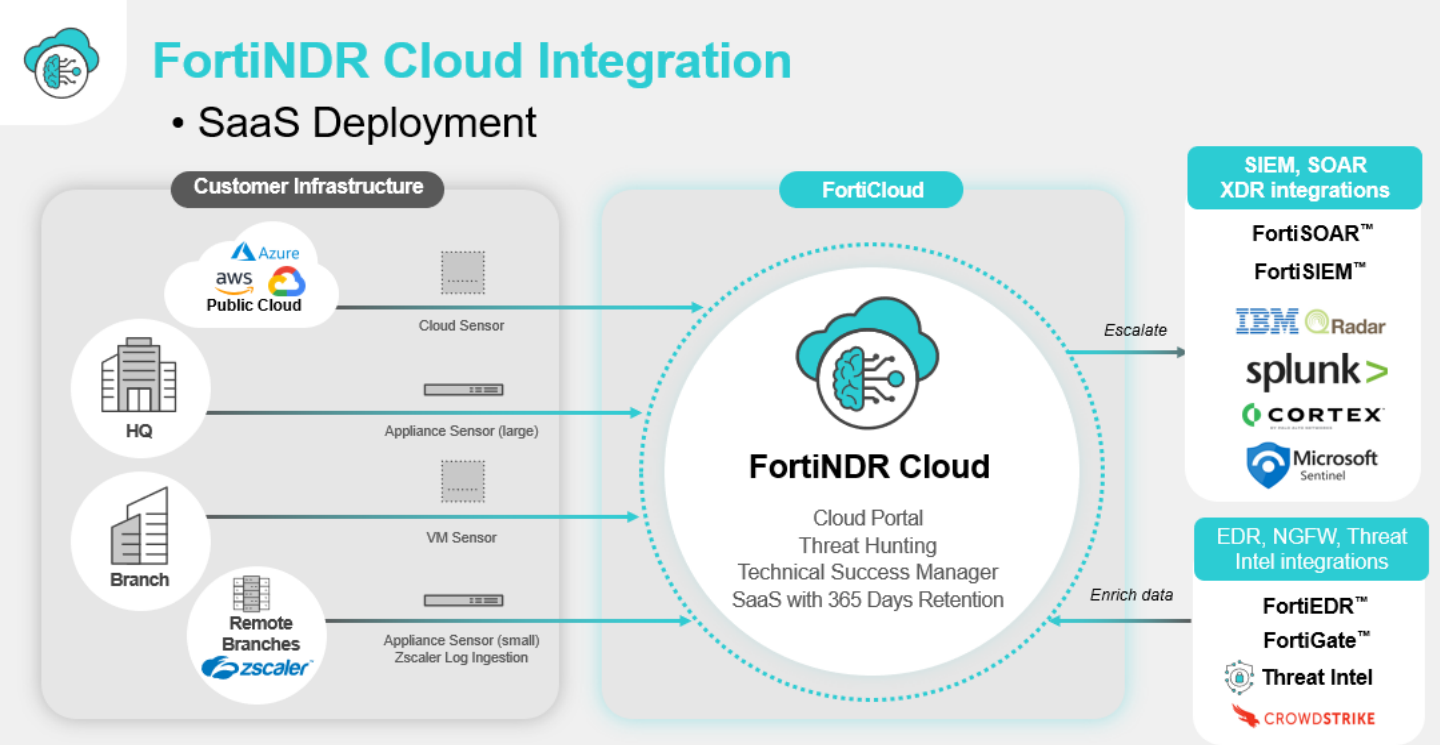
- **FortiNDR Cloud**: processes network traffic in the cloud and provides 365-day retention and advanced network detection and threat hunting functionality. Provides SaaS console for customers to monitor detections and threat hunting.
- **FortiNDR On-premise**: stores and processes all data locally. Nothing leaves the network. Provides local console for customers to log in and manage the solution.

FORTINDR CLOUD

FortiNDR Cloud is a cloud-based SaaS offering that leverages AI, ML, and behavioral and static analysis to assess network traffic and spot threats early in the attack lifecycle.

FortiNDR Cloud includes a Technical Success Manager to assist each deployment and has regular cadence calls with users to optimize solution deployment.

Following is the FortiNDR Cloud architecture diagram:



For hardware sensor technical specifications, see the datasheet.

FORTINDR CLOUD ORDER INFORMATION

SOLUTION BUNDLE	FORTINDR CLOUD-SAAS SERVICES	FORTINDR CLOUD-500F (SMALL SENSOR)	FORTINDR CLOUD 900F (LARGE SENSOR)	FORTINDR CLOUD VIRTUAL SENSORS
FortiNDR Cloud – Base Subscription (includes 1 Gbps throughput)* MANDATORY	FC1-10-NDRCL-667-02-DD*			
Throughput True-up**	NDRC-TRUEUP-1MTH			
Log Ingestion (1000 EPS)***	FC1-10-NDRCL-1009-02-DD			
Sensors Hardware		FNRC-500F	FNRC-900F	Supplied by customer
Sensor Hardware Annual Subscription		FC-10-NDR5F-247-02-DD*	FC-10-NDR9F-247-02-DD*	Free of charge (download from portal)
Sensor Support		FC-10-NDR5F-247-02-DD*	FC-10-NDR9F-247-02-DD*	

* Measure of total throughput by all sensors. For example, five sensors sending a total combined throughput of 10 Gbps throughput requires 10 × 1 Gbps of the SaaS SKU. "DD" specifies the contract length in months. Available terms are 1, 3, and 5 years (i.e. 12, 36, and 60 months). All non-standard terms more than 1 year require coterm
** Not to be used in initial quote/order. True up are used for overages during the contract period. Fortinet reviews and reports usage regularly.
*** Zscaler log ingestion supported. Must be purchased with bandwidth SKU
All initial orders must include cloud services with data throughput. They may purchase hardware sensors to use free virtual sensors to provide data. Additional sensors may be purchased later. Sensor Hardware does not require purchase of additional transceiver.

FORTINDR CLOUD EXAMPLE ORDERS

EXAMPLE OF MINIMAL ORDER:

Monitoring of cloud traffic with < 1 Gb/s bandwidth.

- Cloud services (FC1-10-NDRCL-667-02-12) Two years minimum term recommended.
- AWS Virtual sensor. (Can be downloaded free of charge after cloud services are provisioned.)

EXAMPLE OF MORE COMPLEX ORDER:

Monitoring multiple office locations and cloud traffic along with Zscaler remote access.

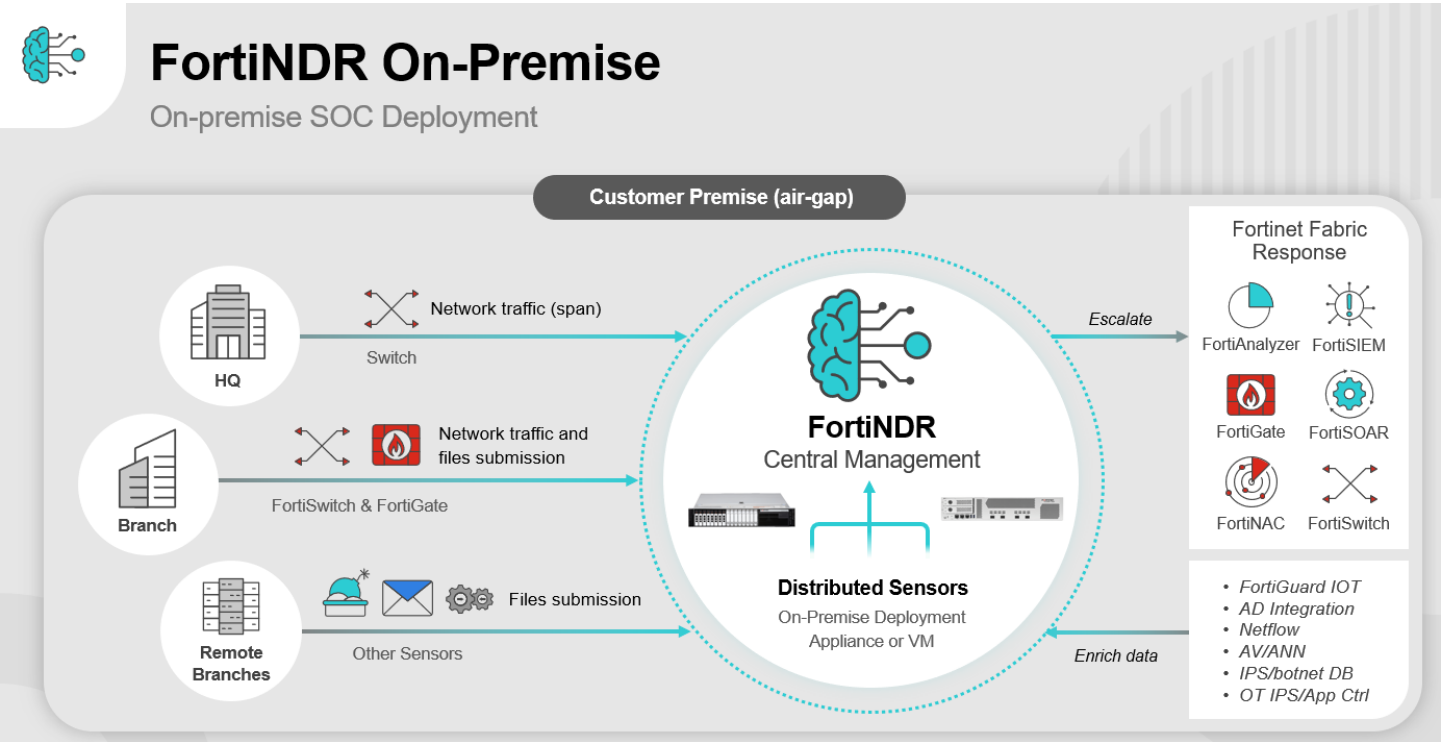
- Total bandwidth: 6 Gb/s
- Zscaler log rate: 3000 EPS
- Term: 3 years
- 2 large physical sensors, 3 virtual sensors

- Cloud services: FC1-10-NDRCL-667-02-36 (x6)
- Large sensors: FNRC-900F (x2)
- Sensor subscription and support: FC-10-NDR9F-247-02-36
- Log ingestion: FC1-10-NDRCL-1009-02-36 (x3)
- Virtual sensors: Downloaded free of charge (x3)

FORTINDR ON-PREMISE

FortiNDR on-premise is suitable for customers with on-premise SOC capacity or to satisfy air-gap or high compliance deployments where all data remains on-premise. Leveraging Fortinet Security Fabric integration, FortiNDR can automatically discover and classify every device communicating across the network, including east/west traffic in the data center. FortiNDR also supports high throughput malware scanning with ANN and supports various Fabric integrations.

Here is a reference architecture diagram with FortiNDR:



FortiNDR on-premise hardware and virtual machines can run in three modes:

- Standalone
- Center (supported on FNR-3600G, FNR-3500F, and Center VM models only)
- Sensors

Center and sensors modes are used for deploying distributed deployment. See the following table or datasheet for mode support for different models.

FORTINDR HARDWARE ORDER INFORMATION

SOLUTION BUNDLE		FORTINDR-1000F	FORTINDR-3500F (GPU ACCELERATED)	FORTINDR-3600G
Hardware Bundles	**Hardware Bundle**	FNR-1000F-BDL-331-DD	FNR-3500F-BDL-331-DD	FNR-3600G-BDL-331-DD
	Renewal	FC-10-AI1KF-331-02-DD	FC-10-AI3K5-331-02-DD	FC-10-AI36G-331-02-DD
Deploy Mode		Standalone, Sensor	Standalone, Center	Center only
Sensors Managed*			Up to 20	25
High Availability Support (for all models)		Active-passive (standalone mode)	Active-passive (standalone mode) Dual center support (center mode)	Dual center support (center mode)
Netflow Support (licensed separately)		FC-10-AI1KF-588-02-DD	FC-10-AI3K5-588-02-DD	FC-10-AI36G-588-02-DD
OT Security Services (licensed separately)		FC-10-AI1KF-723-02-DD	FC-10-AI3K5-723-02-DD	FC-10-AI36G-723-02-DD

In SKUs, "DD" specifies the contract length in months. For example, 12, 36, and 60 are equivalent to 1, 3, and 5 years of support, respectively.
* For cases that require more than 20 sensors, consult Fortinet CSE for details.

DISK ORDERING INFORMATION FOR FORTINDR-3500F

For FortiNDR-3500F, you can use additional disks for expanded capacity. The following table summarizes the disk capacity options for FortiNDR-3500F. FortiNDR-3500F performs better and has longer retention if equipped with more disks/full capacity, especially in center mode where sensors send traffic to center.

Number of SSDs in FNR-3500F	8 (8 × 3.84 TB ship by default)	10	12	14	16
Total capacity (TB) (RAID 10 configuration)	15.36	19.2	23.04	26.88	30.72

FORTINDR VM ORDER INFORMATION

SOLUTION BUNDLE	VM16	VM32	VM CENTER
Deploy Mode	Standalone, Sensor	Standalone, Sensor	Center
Sensors Managed*			Up to 20
High Availability Support (for all models)	Active-passive (standalone mode)	Active-passive (standalone mode)	Dual center support (center mode)
Annual Subscription	FC3-10-AIVMS-461-02-DD	FC4-10-AIVMS-461-02-DD	FC1-10-AIVMC-757-02-DD (up to 10 sensors) FC5-10-AIVMC-757-02-DD (unlimited sensors)
Netflow Support (licensed separately)	FC3-10-AIVMS-588-02-DD	FC4-10-AIVMS-588-02-DD	Licensed on sensors
OT Security Services (licensed separately)	FC3-10-AIVMS-723-02-DD	FC4-10-AIVMS-723-02-DD	

In SKUs, "DD" specifies the contract length in months. For example, 12, 36, and 60 are equivalent to 1, 3, and 5 years of support, respectively.
* For cases that require more than 20 sensors, consult Fortinet CSE for details.

FORTINDR ACCESSORIES

For customers who are running FortiAI 1.5.x and want to enjoy NDR features in v7.0, a co-term upgrade is necessary. Contact customer service at cs@fortinet.com. You can find upgrade information in the Release Notes. Fully populated disks are strongly recommended for managing multiple sensors for data synchronization to center.

FORTINDR APPLIANCE 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 AND FORTINDR CLOUD LICENSING FAQS

Are there any device limits in the FortiNDR On-premise and FortiNDR Cloud solutions?

No, there are no device limits. FortiNDR Cloud, being a SaaS solution, is licensed on bandwidth.

How is FortiNDR Cloud licensed?

FortiNDR Cloud is licensed based on total aggregated bandwidth for all sensors sending traffic to the cloud. For example, five sensors sending 10Gbps to cloud. Physical sensors are ordered separately with support. Virtual sensors are free of charge.

For FortiNDR On-premise, do I need to purchase an additional license when using FNR-3500F as a center to manage sensors?

No, the FNR-3500F can operate in center mode managing sensors with no additional license required for sensor management.

For FortiNDR On-premise, do I need to purchase a Netflow license for center management?

No, netflow is licensed on sensors only. However, if you want to turn FNR-3500F in standalone mode and use netflow features, you should purchase a license.

For FortiNDR On-premise, do I need to purchase an OT license for FNR-3500F center management?

Purchasing OT licenses on FNR-3500F is recommended. Centralized update via center is planned for release in 2024. You can also run FNR-3500F in standalone mode where you may require OT signature updates.

For FortiNDR centralized VM center, what are the differences between the two center VM SKUs?

The difference is in the number of devices managed. SKU FC1-10-AIVMC-757-02-DD can allow management of up to ten devices, and SKU SKU FC5-10-AIVMC-757-02-DD can allow management of unlimited sensors.

For FortiNDR centralized VM center, what if I need an upgrade to manage more than ten sensors?

You will need to purchase a new subscription of unlimited sensors.

Visit www.fortinet.com for more details