



FortiEDR

Product Offerings

Endpoint Detection and Response (EDR) subscription bundles are available for different use cases, depending on the customer needs, other Fortinet Security Fabric products deployed, as well as managed service options. The following table summarizes the most common and recommended options:

	EDR-LIGHT	EDR	XDR
	DISCOVER AND PROTECT	DISCOVER, PROTECT, AND RESPOND	DISCOVER, PROTECT, AND RESPOND WITH XDR
IT Hygiene			
Asset Discovery	✓	✓	✓
Asset Assessment	✓	✓	✓
Attack Surface Reduction	✓	✓	✓
Application Control	✓	✓	✓
USB Control	✓	✓	✓
Endpoint Protection			
NGAV (pre-execution)	✓	✓	✓
Post-execution Protection	✓	✓	✓
Cloud Sandbox	✓	✓	✓
Cloud Threat Intelligence	✓	✓	✓
Attack Chain Visualization	✓	✓	✓
Web Filtering	✓	✓	✓
Endpoint Detection and Response			
Advanced Forensics	✓	✓	✓
MITRE Tagging	✓	✓	✓
AI-powered Investigation	✓	✓	✓
Automated Integrative Incident Response	✓	✓	✓
Secured Remote Shell	✓	✓	✓
Continuous Recording and Analysis		✓	✓
Threat Hunting		✓	✓
AI-based Behavior Tagging		✓	✓
IOC Ingestion and Search		✓	✓
eXtended Detection and Response			
Security Fabric Integrated			✓
Detection Across Security Fabric			✓
Automated Playbook Investigation			✓
Automated Remediation			✓
Third Party Support			✓
Managed Service Options			
High Fidelity Alert Triage	Managed EDR	Managed EDR	Managed XDR
Extended Alert Triage		Managed EDR	Managed XDR
Containment and Remediation Guidance		Managed EDR	Managed XDR
Alerting and Reporting		Managed EDR	Managed XDR
Correlated Security Fabric Alert Triage			Managed XDR
Additional Services			
24x7 Support	Included	Included	Included
Deployment	Cloud	On-premise Internet access enabled	Cloud

To download datasheets, product matrices, and case studies, go to <https://www.fortinet.com/products/endpoint-security/fortiedr>.



ORDER INFORMATION

FortiEDR is available in flexible combinations. For the best security coverage, the all-in-one subscription is recommended.

DISCOVER, PROTECT, AND RESPOND				
	EDR	XDR	Managed EDR	Managed XDR
25-pack	FC1-10-FEDR1-348-01-DD	FC1-10-FEDR1-394-01-DD	FC1-10-FEDR1-349-01-DD	FC1-10-FEDR1-396-01-DD
500-pack	FC2-10-FEDR1-348-01-DD	FC2-10-FEDR1-394-01-DD	FC2-10-FEDR1-349-01-DD	FC2-10-FEDR1-396-01-DD
2,000-pack	FC3-10-FEDR1-348-01-DD	FC3-10-FEDR1-394-01-DD	FC3-10-FEDR1-349-01-DD	FC3-10-FEDR1-396-01-DD
10,000-pack	FC4-10-FEDR1-348-01-DD	FC4-10-FEDR1-394-01-DD	FC4-10-FEDR1-349-01-DD	FC4-10-FEDR1-396-01-DD

For customers in the process of migrating from a traditional endpoint protection platform or next generation antivirus solution towards EDR, a basic Discover and Protect option is available, which supports future migration to full EDR.

DISCOVER AND PROTECT		
	EDR-Light	Managed EDR
25-pack	FC1-10-FEDR1-350-01-DD	FC1-10-FEDR1-391-01-DD
500-pack	FC2-10-FEDR1-350-01-DD	FC2-10-FEDR1-391-01-DD
2,000-pack	FC3-10-FEDR1-350-01-DD	FC3-10-FEDR1-391-01-DD
10,000-pack	FC4-10-FEDR1-350-01-DD	FC4-10-FEDR1-391-01-DD

Additional services available include expanded cloud storage, NSE training, professional services, and best practice deployment consultation.

ADDITIONAL SERVICES	SERVICES	SKU LICENSE
Cloud Storage	Disk Expansion (512 GB storage)	FC-10-FEDR0-344-01-DD
	Less than 1,000 endpoints	FC1-10-EDBPS-310-02-DD
	1,000 to 3,000 endpoints	FC2-10-EDBPS-310-02-DD
	3,000 to 10,000 endpoints	FC3-10-EDBPS-310-02-DD
	10,000 to 30,000 endpoints	FC5-10-EDBPS-310-02-DD
FortiCare Best Practices Onboarding Service (mandatory for onboarding customers)	30,000 or more endpoints	FP-10-EDR-PS (per day)
	FortiEDR Professional Service	FP-10-FTEDR-000-00-00
	FortiEDR Day	FP-10-EDR-PS
	Incident Response Training	FP-10-PS-TRAINING
Professional Services	Forensics and IR Consultancy	FP-10-EDR-FRNCS
	Classroom - Virtual ILT	FT-EDR
Training Services	Lab Access - Standard NSE Training Lab Environment	FT-EDR-LAB
	NSE5 Exam Voucher	NSE-EX-SPL5

SEE ALSO

Other FortiEDR SKUs are orderable for the following deployments. See the FortiEDR datasheet for information about these deployments:

- **Protect and Respond (P&R):** for special cases where customers may have complimentary vulnerability discovery in place already, a special subscription is available. This subscription supports the standard XDR, MDR, and MXDR variations.
- **On-premise:** for special deployments, an on-premise hosting option with FortiGuard Cloud Services (FCS) connection enabled is available.



ORDER LIFECYCLE

<p>New Order <i>Example: 500 EDR endpoints</i></p> <p>Direct purchase 1x500-pack</p> <ul style="list-style-type: none"> FC2-10-FEDR1-348-01-12 FC1-10-EDBPS-310-02-DD <p>Add More Endpoints <i>Example: add 50 EDR endpoints</i></p> <p>Use the co-term tool to add more endpoints and align the end dates:</p> <ul style="list-style-type: none"> FC1Z-15-FEDR1-348-02-00 (x2) 	<p>Renew All Endpoints <i>Example: renew all 550 EDR endpoints</i></p> <p>Regardless of the option used above, use the co-term tool for all renewals. This aligns all contracts to the same expiration date.</p> <ul style="list-style-type: none"> FC1Z-15-FEDR1-348-02-00 (x2) FC2Z-15-FEDR1-348-02-00 (x1) <p>Upgrade All Endpoints <i>Example: upgrade all 550 EDR endpoints to XDR</i></p> <p>Use the co-term tool to upgrade all endpoints to the end of the term, then follow standard renewal:</p> <ul style="list-style-type: none"> FC1Z-15-FEDR1-394-02-00 (x2) FC2Z-15-FEDR1-394-02-00 (x1)
--	---

UPGRADE MATRIX

FortiEDR contains three subscriptions, and each subscription contains multiple different service levels. You can convert one subscription to another in two steps:

1. Change the subscription level if required
2. Change the service level if required

To use the upgrade matrix below:

1. Select your current version in the left column
2. Locate the desired version column

If the cell is blue, you can upgrade in one step using the co-term tool. If not, you may need to complete two steps.

Upgrade FROM	UPGRADE TO													
	Discover and Protect		Protect and Respond				Discover, Protect, and Respond				On-premise			
	EPP/NGAV	Managed AV	EDR	XDR	MDR	MXDR	EDR	XDR	MDR	MXDR				
EPP/NGAV	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Managed AV	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
EDR (P&R)	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
XDR (P&R)	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
MDR (P&R)	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
MXDR (P&R)	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
EDR	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
XDR	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
MDR	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
MXDR	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue

To use this matrix, select the **current** subscription in the left column and follow the row to the right to see what is **directly upgradable** with the co-term tool.



FREQUENTLY ASKED QUESTIONS

What is the easiest way to order?

License packs of 25, 500, 2,000, and 10,000 are available for terms of 1-5 years. Refer to the ordering example on the previous page for expansions, renewals, and upgrades.

Does FortiEDR have a minimum order quantity (MOQ)?

The MOQ is 500 seats for all bundles except for a single blended bundle, FC1-10-FEDR1-349-01-DD + FC1-10-EDBPS-310-02-DD, which allows 100 seats.

Can I mix bundles?

No. FortiEDR supports a single bundle per customer account.

Can existing customers upgrade bundles?

Yes. Customers can upgrade at any point of time: mid-term or upon renewal.

What if my customer is a managed security service provider (MSSP)?

Checking the MSSP Ordering Guide is recommended. MSSP consumption plans are available on an annual or monthly billing basis.

What services can be provided to an on-premise environment?

On-premise hosted environments require Fortinet Cloud Services Internet connectivity at all times. Once connected, all FortiEDR-related services can be delivered remotely. FortiEDR does not support air-gapped isolated on-premise-hosted environments.

Onboarding

Is a FortiEDR onboarding service required?

Yes. Proper EDR setup is crucial for security effectiveness plus system outage avoidance or SOC overload. The onboarding processes include monitoring and finetuning of critical assets/resources.

What onboarding options are available?

The following summarizes standard onboarding engagement with the FortiCare Best Practice Service. Dedicated professional services for SLA-driven engagements are also available and required for deployments with more than 30,000 endpoints.

SIZE	INCLUDED	SERVICE ENGAGEMENT WORKFLOW
< 1,000	<ul style="list-style-type: none"> 4 hours dedicated review (1 per week) 30 days analyst monitoring 1 year subscription for upgrades and add-on support 	<ol style="list-style-type: none"> Service kickoff includes platform overview and customer infrastructure review leading to customer's deployment plan. Best practice advice during deployment and migration includes scheduled service meetings, responding to ad-hoc questions, reviewing alerts received, and reviewing and making recommendations regarding the ongoing methodology for the customer to migrate the collectors to protection mode. Final deployment closeout meeting.
1,000 - 2,999	<ul style="list-style-type: none"> 12 hours dedicated review (1 per week) 90 days analyst monitoring 1 year subscription for upgrades and add-on support 	
3,000-9,999	<ul style="list-style-type: none"> 16 hours dedicated review (1 per week) 120 days analyst monitoring 1 year subscription for upgrades and add-on support 	
10,000-29,999	<ul style="list-style-type: none"> 24 hours dedicated review (1 per week) 180 days analyst monitoring 1 year subscription for upgrades and add-on support 	
>= 30,000	Dedicated professional services (PS) required	

