ORDERING GUIDE

FortiEDR/FortiXDR

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:

		EPP/EDR-LIGHT	EDR	XDR
		DISCOVER AND PROTECT	DISCOVER, PROTECT, AND RESPOND	DISCOVER, PROTECT, AND RESPOND WITH XDR
Discover	**IT Hygiene**			
	Asset Discovery	✓	✓	✓
	Asset Assessment	✓	✓	✓
	Attack Surface Reduction	✓	✓	✓
	Application Control	✓	✓	✓
	USB Device Control	✓	✓	✓
Protect	**Endpoint Protection**			
	NGAV (pre-execution)	✓	✓	✓
	Post-execution Protection	✓	✓	✓
	Sandbox Analysis	✓	✓	✓
	Cloud Threat Intelligence	✓	✓	✓
	Attack Chain Visualization	✓	✓	✓
	Advanced Incident Forensics	✓	✓	✓
	MITRE Tagging	✓	✓	✓
Respond	**Endpoint Detection and Response**			
	AI-powered Investigation	✓	✓	✓
	Security Fabric Integration	✓	✓	✓
	Third-Party Integration	✓	✓	✓
	Automated Remediation and IR Framework	✓	✓	✓
	Secured Remote Shell	✓	✓	✓
	Continuous Recording and Analysis		✓	✓
	Threat Hunting Enablement		✓	✓
	AI-based Behavior Tagging		✓	✓
	IOC Ingestion and Search		✓	✓
XDR	**eXtended Detection and Response**			
	eXtended Detection Across Security Fabric			✓
	eXtended Detection Across AWS Guard-Duty			✓
	eXtended Detection Across Google SCC			✓
MDR	**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	24×7 Support	Included	Included	Included
	Cloud Deployment	Supported	Supported	Supported
	On-premise Internet access enabled		Supported	

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

Sample Bundles	EPP/EDR-Basic	EDR-Complete	XDR
25-pack	FC1-10-FEDR1-350-01-DD	FC1-10-FEDR1-348-01-DD	FC1-10-FEDR1-394-01-DD
500-pack	FC2-10-FEDR1-350-01-DD	FC2-10-FEDR1-348-01-DD	FC2-10-FEDR1-394-01-DD
2,000-pack	FC3-10-FEDR1-350-01-DD	FC3-10-FEDR1-348-01-DD	FC3-10-FEDR1-394-01-DD
10,000-pack	FC4-10-FEDR1-350-01-DD	FC4-10-FEDR1-348-01-DD	FC4-10-FEDR1-394-01-DD

Managed service options are available for all endpoint protection options, however cannot be supported for on-prem deployments.

Sample Bundles	Managed EPP/EDR-Basic	Managed EDR-Complete	Managed XDR
25-pack	FC1-10-FEDR1-391-01-DD	FC1-10-FEDR1-349-01-DD	FC1-10-FEDR1-597-01-DD
500-pack	FC2-10-FEDR1-391-01-DD	FC2-10-FEDR1-349-01-DD	FC2-10-FEDR1-597-01-DD
2,000-pack	FC3-10-FEDR1-391-01-DD	FC3-10-FEDR1-349-01-DD	FC3-10-FEDR1-597-01-DD
10,000-pack	FC4-10-FEDR1-391-01-DD	FC4-10-FEDR1-349-01-DD	FC4-10-FEDR1-597-01-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-FEDR1-1112-01-DD
FortiCare Best Practices Onboarding Service (mandatory for onboarding customers)[1]	**Up to 500 endpoints**	FC0-10-EDBPS-310-02-DD
	501 to 1,000 endpoints	FC1-10-EDBPS-310-02-DD
	1,001 to 3,000 endpoints	FC2-10-EDBPS-310-02-DD
	3,001 to 10,000 endpoints	FC3-10-EDBPS-310-02-DD
	10,001 to 30,000 endpoints	FC5-10-EDBPS-310-02-DD
	30,001 or more endpoints	FP-10-EDR-PS (per day)
Professional Services	**FortiEDR Professional Service**	FP-10-FTEDR-000-00-00
	FortiEDR Day	FP-10-EDR-PS
	Incident Response Training	FP-10-PS-TRAINING
	Forensics and IR Consultancy	FP-10-EDR-FRNSCS
Training Services	**Classroom - Virtual ILT**	FT-EDR
	Lab Access - Standard NSE Training Lab Environment	FT-EDR-LAB
	NSE5 Exam Voucher	NSE-EX-SPL5

1 All new customers (initial orders only) must include one of the Best Practices service SKUs. Select the package that matches the total number of the deployment (e.g. FC3-10EDB-PS-310-02-12 for a deployment of 6450 seats). In most situations, anything over 12 months is not necessary. Use the 12 month SKU in all new deals unless requested by customer.

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

New Order

Example: 500 EDR endpoints

Direct purchase 1×500-pack

- FC2-10-FEDR1-348-01-12
- FC0-10-EDBPS-310-02-DD

Add More Endpoints

Example: add 50 EDR endpoints

Use the co-term tool to add more endpoints and align the end dates:

- FC1Z-15-FEDR1-348-02-00 (x2)

Renew All Endpoints

Example: renew all 550 EDR endpoints

Regardless of the option used above, use the co-term tool for all renewals. This aligns all contracts to the same expiration date.

- FC1Z-15-FEDR1-348-02-00 (x2)
- FC2Z-15-FEDR1-348-02-00 (x1)

Upgrade All Endpoints

Example: upgrade all 550 EDR endpoints to XDR

Use the co-term tool to upgrade all endpoints to the end of the term, then follow standard renewal:

- 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 TO										
	Discover and Protect		Protect and Respond				Discover, Protect, and Respond				
Upgrade FROM	EDR-Light	Managed EDR-Light	EDR	XDR	MDR	MXDR	EDR	XDR	MDR	MXDR	On-premise
EDR-Light											
Managed EDR-Light											
EDR (P&R)											
XDR (P&R)											
MDR (P&R)											
MXDR (P&R)											
EDR											
XDR											
MDR											

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.

NSE TRAINING AND CERTIFICATION

FCP – FortiEDR Training and Certification

Learn how to use FortiEDR to protect your endpoints against advanced attacks with real-time orchestrated incident response functionality. You will also explore FortiEDR features and how they protect your endpoints automatically in real time.

Course Description

For more information about prerequisites, agenda topics and learning objectives, please refer to the course description at https://training.fortinet.com/local/staticpage/view.php?page=library_fortiedr

Ordering Information

SKU	DESCRIPTION
FT-EDR	Instructor-led Training - 2 full days or 3 half days
FT-EDR-LAB	On-demand Labs (self-paced)
NSE-EX-FTE2	Certification Exam

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 the FortiEDR Discover & Protect, the 350 family of SKUs which allows 250 seats, the FortiEDR Discover & Protect and Basic MDR, the 391 family of SKUs which allows 100 seats, the FortiEDR Protect & Respond and Standard MDR, the 392 family of SKUs which allows 100 seats and the FortiEDR Discover, Protect & Respond and Standard MDR, the 349 family of SKUs which allows 100 seats. That said, positioning 500 seats for smaller seat accounts who can manage their incident response is a valid option.

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, except for MDR service. FortiEDR does not support air-gapped isolated on-premise-hosted environments.

What is FortiEndpoint?

FortiEndpoint is Fortinet's unified agent that combines FortiClient and FortiEDR. It provides a comprehensive solution through a single SKU that includes secure connectivity options (VPN or ZTNA), as well as Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) capabilities.

For more information, please visit FortiEndpoint Ordering Guide.

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. Onboarding is not required for renewals.

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
<= 1000	• 4 hours dedicated review (1 per week) • 30 days analyst monitoring • 1 year subscription for upgrades and add-on support	1. **Service kickoff** includes platform overview and customer infrastructure review leading to customer's deployment plan. 2. **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. 3. **Final deployment** closeout meeting.
1,001 - 3,000	• 12 hours dedicated review (1 per week) • 90 days analyst monitoring • 1 year subscription for upgrades and add-on support	
3,001 - 10,000	• 16 hours dedicated review (1 per week) • 120 days analyst monitoring • 1 year subscription for upgrades and add-on support	
10,001 - 30,000	• 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	

Visit www.fortinet.com for more details

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.