

FortiDLP



FortiDLP is a combined endpoint data loss prevention (DLP) and insider risk management solution and a key component of Fortinet's data security offerings. FortiDLP continuously monitors endpoint and corporate cloud drive activity and user behavior to detect and prevent accidental data loss and deliberate data exfiltration. The solution addresses data security compliance requirements with out-of-the-box support for data privacy legislation and industry regulations.

FortiDLP offers the following tiers:

- **Standard:** gain immediate visibility and control over data movement on your endpoints to guard against data misuse and loss. The Standard license includes core data loss prevention features. It is ideal for organizations that want to manage data security risks and address regulatory compliance.
- **Enterprise:** caters to organizations running DLP and insider risk management programs. In addition to DLP, it provides extensive user, data, and file activity event streams. It adds machine learning-powered user behavior monitoring, MITRE ATT&CK®-mapped insider threat sequence detection, screenshot forensics capture, and enterprise cloud drive integrations to provide visibility and detection for cloud drive activity, including downloads and file sharing.
- **Enterprise Premium:** same as Enterprise tier with support for premium PoP hosting locations, such as the Kingdom of Saudi Arabia (KSA).

FortiDLP also offers a Best Practices Service (BPS) and a Managed Service where Fortinet experts work as an extension of your security team to help set up, optimize, and provide ongoing management and monitoring of data security risks across the organization.

Product Offerings

The following table summarizes the features included in each license tier. All tiers are delivered from our cloud-native SaaS solution:

	STANDARD	ENTERPRISE	MANAGED
FEATURES			
DLP			
Device Control	✓	✓	✓
Inline DLP for Web, Email, Printers, Clipboard and Removable Media	✓	✓	✓
Real-time Content Inspection (On and Off Network)	✓	✓	✓
Data Loss Prevention Based on Data Source (e.g. Salesforce and GitHub)	✓	✓	✓
GenAI and SaaS Application Risk Inventory and Data Flow Analytics	✓	✓	✓
Customized Employee Coaching with Response Telemetry	✓	✓	✓
Data Privacy and Regulatory Compliance Global Policy Library	✓	✓	✓
Microsoft Purview Sensitivity Label Support	✓	✓	✓
Evidence Store Support for File and Clipboard Forensics	✓	✓	✓
Incident Management and DLP Activity Timeline	✓	✓	✓
Dynamic Risk Adaptive Policies	✓	✓	✓
INSIDER RISK			
Immediate Visibility into User and Data Risks Across Endpoints and Enterprise Cloud Drives		✓	✓
MITRE ATT&CK®-mapped Insider Threat Detection Library	✓		✓
Insider Threat Data Exfiltration Sequence Detection	✓		✓
Machine Learning-Powered Behavior Analytics	✓		✓
Data Lineage Tracking with File Manipulation Detection	✓		✓
Endpoint Isolate and Lock Actions	✓		✓
Evidence Store Support for File, Clipboard and Screen Capture Forensics	✓		✓
Case Management	✓		✓
ENTERPRISE CLOUD INTEGRATION			
Microsoft Office 365 Connector	✓		✓
Google Workspace Connector	✓		✓
Box Drive Connector	✓		✓
Real-time Employee Coaching via Slack and Teams Messaging	✓		✓
Support for M365 (Purview), Google, and Box Classification Labels	✓		✓
File Sharing Controls	✓		✓
MANAGED SERVICE			
Product Configuration and Provisioning		✓	
Monthly Data Reports and Security Analyst Reviews		✓	
DLP Policy Optimization		✓	
Incident Monitoring Assistance		✓	
Product Change Management		✓	

Available Services for FortiDLP

The following table indicates what customers can expect to get from FortiCare Premium support and Best Practices and Managed Services.

FEATURES	SUPPORT	ADDITIONAL EXPERT SERVICES	
	FORTICARE PREMIUM SUPPORT*	BPS**	MANAGED SERVICE**
TECHNICAL SUPPORT			
Reponse Time (Critical Issues)	1 hour		
Response Time (Non-Critical Issues)	Next business day		
Phone Support	✓		
Web Support	✓		
SERVICES			
FortiDLP Setup	✓	✓	✓
Designated FortiDLP Contact	✓	✓	✓
FortiDLP Best Practice Advice	✓	✓	✓
Checkpoint Meetings (Remote)	✓	✓	✓
FortiDLP Console Configuration and Change Management		✓	
Monthly FortiDLP Data Reports and Reviews (Remote)		✓	
Annual FortiDLP Product Configuration Review (Remote)		✓	

*Included with Standard and Enterprise licensing subscriptions. For more information refer to [FortiCare Services](#).

**Mandatory BPS or Managed Service purchase in the first FortiDLP subscription year.

Order Information

SOLUTION	DESCRIPTION	NUMBER OF ENDPOINTS	SKU	MOQ
Standard - Endpoint DLP	Cloud-native Endpoint DLP with FortiCare Premium	100-499	FC2-10-DLPEP-1097-02-DD	
		500-1999	FC3-10-DLPEP-1097-02-DD	
		2000-9999	FC4-10-DLPEP-1097-02-DD	
		10000+	FC5-10-DLPEP-1097-02-DD	
Enterprise - Endpoint DLP with Insider Risk and cloud drive integration	Includes cloud-native Endpoint DLP, Insider Risk, and SaaS integration with FortiCare Premium	100-499	FC2-10-DLPEP-1098-02-DD	100
		500-1999	FC3-10-DLPEP-1098-02-DD	
		2000-9999	FC4-10-DLPEP-1098-02-DD	
		10000+	FC5-10-DLPEP-1098-02-DD	

Order Information - Managed Service

SOLUTION	DESCRIPTION	NUMBER OF ENDPOINTS	SKU	MOQ
Managed - Endpoint DLP with Insider Risk and cloud drive integration	Managed cloud-native Endpoint DLP, Insider Risk, and SaaS integration with FortiCare Premium. Includes FortiCare Best Practices Service and Premium PoP location support	100-499	FC2-10-DLPEP-1099-02-DD	
		500-1999	FC3-10-DLPEP-1099-02-DD	
		2000-9999	FC4-10-DLPEP-1099-02-DD	100
		10000+	FC5-10-DLPEP-1099-02-DD	

Order Information - BPS

SOLUTION	NUMBER OF ENDPOINTS/USERS	SKU
FortiCare Best Practices Consultation Service (BPS)*	Up to 999	FC1-10-DLBPS-310-02-DD
	1000-9999	FC2-10-DLBPS-310-02-DD
	10000+	FC3-10-DLBPS-310-02-DD

* The BPS service is required at a minimum for all new customers. New customers can opt for the BPS or Managed Service to satisfy this requirement.



Order Information - Enterprise Premium Service

SOLUTION	DESCRIPTION	NUMBER OF ENDPOINTS/USERS	SKU	MOQ
Enterprise Premium - Endpoint DLP with Insider Risk and cloud drive integration on premium PoP	Cloud-native Endpoint DLP, Insider Risk and SaaS integration on premium PoP location with FortiCare Premium	Up to 499	FC2-10-DLPEP-1174-02-DD	
		500-1999	FC3-10-DLPEP-1174-02-DD	100
		2000-9999	FC4-10-DLPEP-1174-02-DD	
		10000+	FC5-10-DLPEP-1174-02-DD	



Frequently Asked Questions

Which PoPs (hosting regions) require the FortiDLP Enterprise Premium license?

Deployment in the Kingdom of Saudi Arabia (KSA) requires the FortiDLP Enterprise Premium license. The managed service option is not available in KSA.

Is BPS mandatory for FortiDLP?

BPS is mandatory for new customers for the first year so that our customer success team and product experts can help guide customers through deployment and solution configuration. After the first year, BPS is optional. Customers can also opt for the Managed Service.

Does the Managed FortiDLP license include BPS?

The managed service license does not require purchasing BPS separately. The managed service license includes BPS.

Alongside visibility and detection for managed endpoints, does FortiDLP provide visibility and detection for activity in enterprise cloud drives?

Yes. FortiDLP Enterprise, Enterprise Premium, and Managed licenses provide Microsoft OneDrive/SharePoint, Google Drive(Workspace), and Box cloud drive connectors. These connectors audit, track, and detect data sharing and download activities across managed and unmanaged devices with corporate cloud drive systems access.

Does FortiDLP support on-premise deployment or is it only available in the cloud?

FortiDLP is a cloud-native multitenant SaaS solution. There is no on-premise deployment option. FortiDLP does support on-premise evidence store forensics storage.

What options are available for file shadow forensics storage?

With file shadowing, you own and manage your data. Shadow file copies do not upload to the FortiDLP infrastructure. Shadow copies only upload to your chosen storage location, which the FortiDLP agent accesses directly. Your data is protected in motion and at rest. You can store file shadow copies on-premise with MinIO or on the cloud with Amazon Web Services, Google Cloud Storage, or Microsoft Azure Blob Storage.

Does FortiEndpoint include FortiDLP?

FortiDLP is not yet available in the FortiEndpoint (FortiClient unified agent) solution.

Does FortiDLP support integration with SIEM and SOAR products?

FortiDLP provides out-of-the-box support for FortiSIEM, Splunk, and Microsoft Sentinel SIEMs, as well as FortiSOAR and third-party SOAR solutions. By configuring event streaming, webhooks, and/or APIs, you can integrate FortiDLP with all modern SIEM and SOAR solutions.



www.fortinet.com