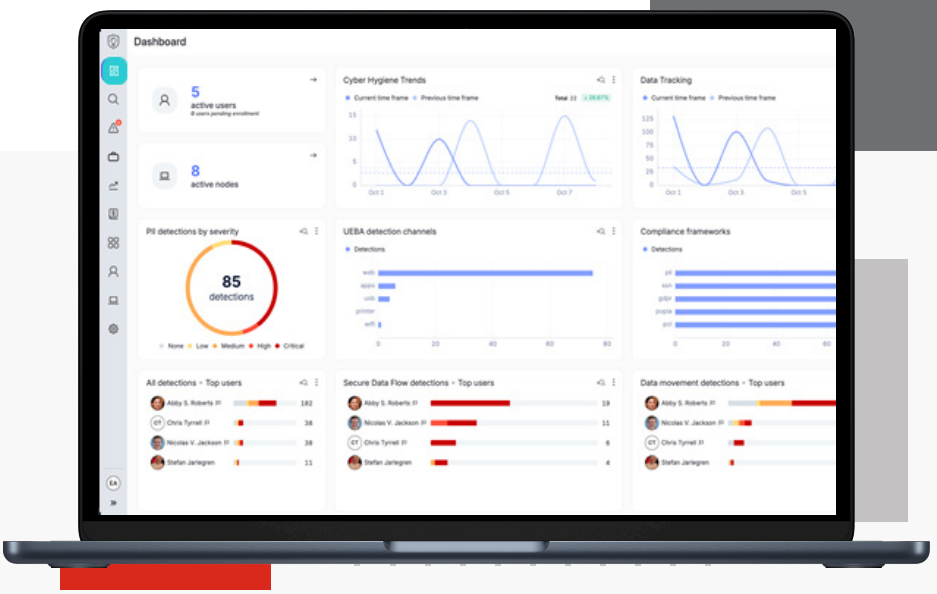
FortiDLP

Next Generation DLP Enhanced by AI



Key Use Cases

- Get real-time visibility into user interactions with sensitive data
- Prevent data loss from exfiltration and accidental leakage
- Monitor for insider threats and high-risk employees
- Secure data in use by SaaS and other applications
- Identify Shadow AI usage and stop the upload of sensitive data
- Apply user and entity behavioral analysis at scale
- Educate users on proper data handling
- Satisfy data security controls associated with major compliance frameworks

Unified DLP, Insider Risk Management, and GenAI Data Protection to Anticipate and Prevent Data Theft

Overview: securing data from insider threats and risks

Today's most valuable currency is data. Whether it's intellectual property, financial account details, patient records, or customer cardholder information, data must be protected from theft or exposure by threat actors, malicious insiders, and careless or untrained employees.

FortiDLP is a unified data loss prevention and insider risk management solution that helps your security team anticipate and prevent data leaks, detect behavior-related insider risks, and train employees on proper cyber hygiene at the point of access to sensitive data including intellectual property—starting from day one. With FortiDLP, your organization gains immediate and full visibility into business data flows and usage across endpoints, enterprise cloud drives, GenAI tools, SaaS apps and other points of egress, allowing teams to detect high-risk activity across users, stop the exfiltration or leakage of sensitive data, and drive prioritized investigations.

Challenges: traditional DLP fails to deliver in today's world

Legacy DLP tools address modern data security challenges with cumbersome data classification and complex static policies before offering any visibility into data loss risks or controls to mitigate them. As a result, data security teams are overburdened by constant policy creation and tuning, inefficient data classification, false positives, and noisy alarms.

FortiDLP overcomes these legacy DLP challenges. FortiDLP baselines individual user behavior (through machine learning embedded in the FortiDLP lightweight agent) and combines localized real-time context and content-level inspection to classify data at the point of access by employees. And unlike legacy solutions, FortiDLP doesn't require exhaustive data discovery or policy formulation before it can provide actual data protection value.

Available in

Cloud

Our Approach

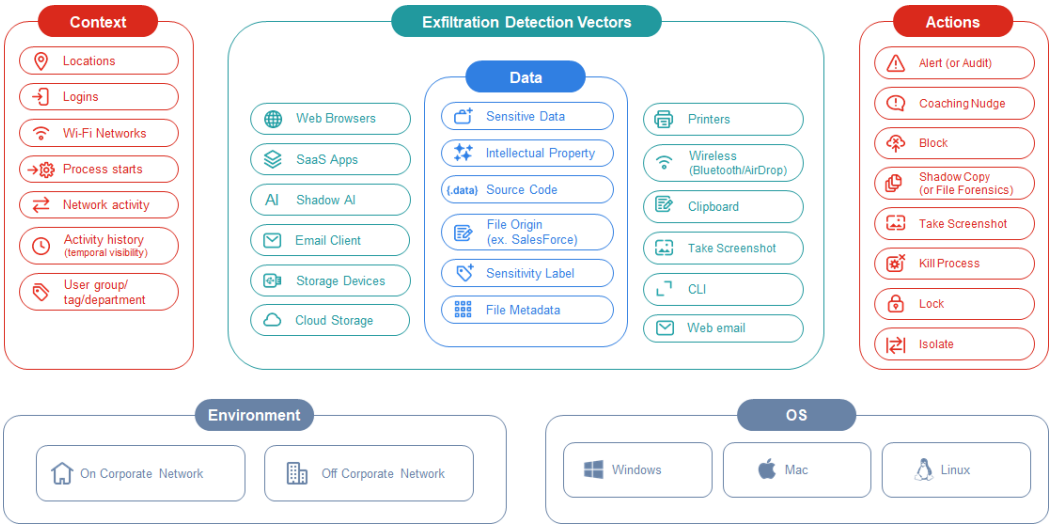
A powerful integrated approach to data loss prevention

FortiDLP delivers a modern, unified approach to data security by combining data loss prevention, insider risk management, GenAI and SaaS data protection, and risk-informed user education.

It provides real-time visibility into data movement and activity across endpoints, cloud storage, SaaS applications—including GenAI tools—and collaboration platforms. This visibility empowers organizations to assess risk and enforce DLP and insider threat policies through proactive, real-time actions.

The FortiDLP lightweight, scalable agent operates independently of network connection or user location, ensuring continuous data flow protection whether employees are in the office, working remotely, or on the move. It also supports enterprise cloud drives such as Microsoft 365, Google Workspace, and Box, and integrates with major messaging systems to enable remediation workflows.

Unlike traditional solutions, FortiDLP avoids sending sensitive business data to cloud-based scanning engines—reducing bandwidth usage and helping meet data residency requirements—while still delivering comprehensive, modern data protection.



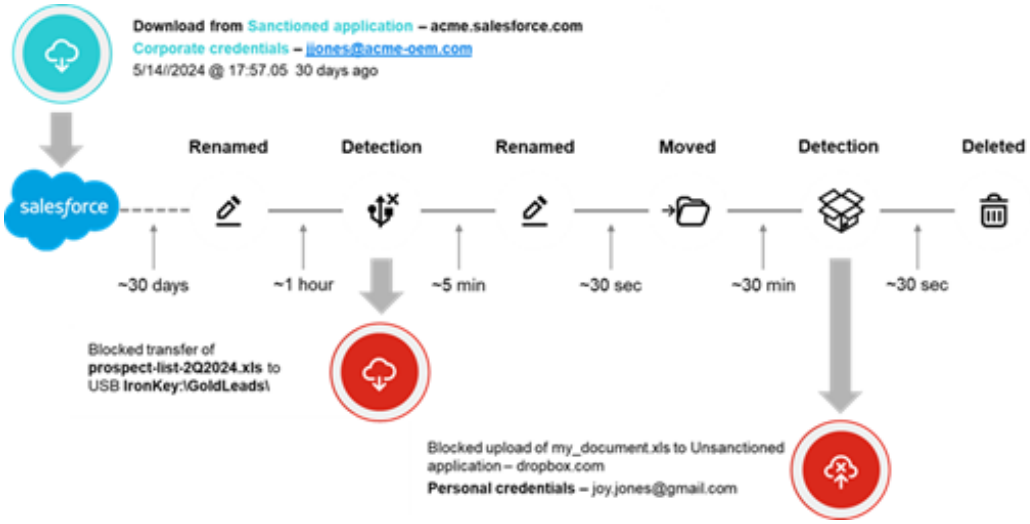
Enhanced with Artificial Intelligence

From day one, FortiDLP applies machine learning—integrated into FortiDLP's agent—to baseline individual user activity and uses behavioral analytics algorithms to detect typical versus novel or anomalous behavior. Additional powerful analysis and analytics capabilities provide insights at an organizational level.

In addition, FortiDLP utilizes FortiAI (AI Assistant) to summarize and contextualize data associated with high-risk activity to accelerate incident analysis. Activities are mapped to MITRE ENGENUITY™ Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base.

Track data from its origin and subsequent manipulations

Through Secure Data Flow and Data Lineage features, FortiDLP can also automatically identify and track data based on its origin, such as Workday or a source code repository. DLP and insider risk policies can be enforced based on where the data originated and whether a corporate or non-corporate account was used to egress data.



Enhanced with Artificial Intelligence

From day one, FortiDLP applies machine learning—integrated into the FortiDLP agent—to baseline individual user activity and uses behavioral analytics algorithms to detect typical versus novel or anomalous behavior.

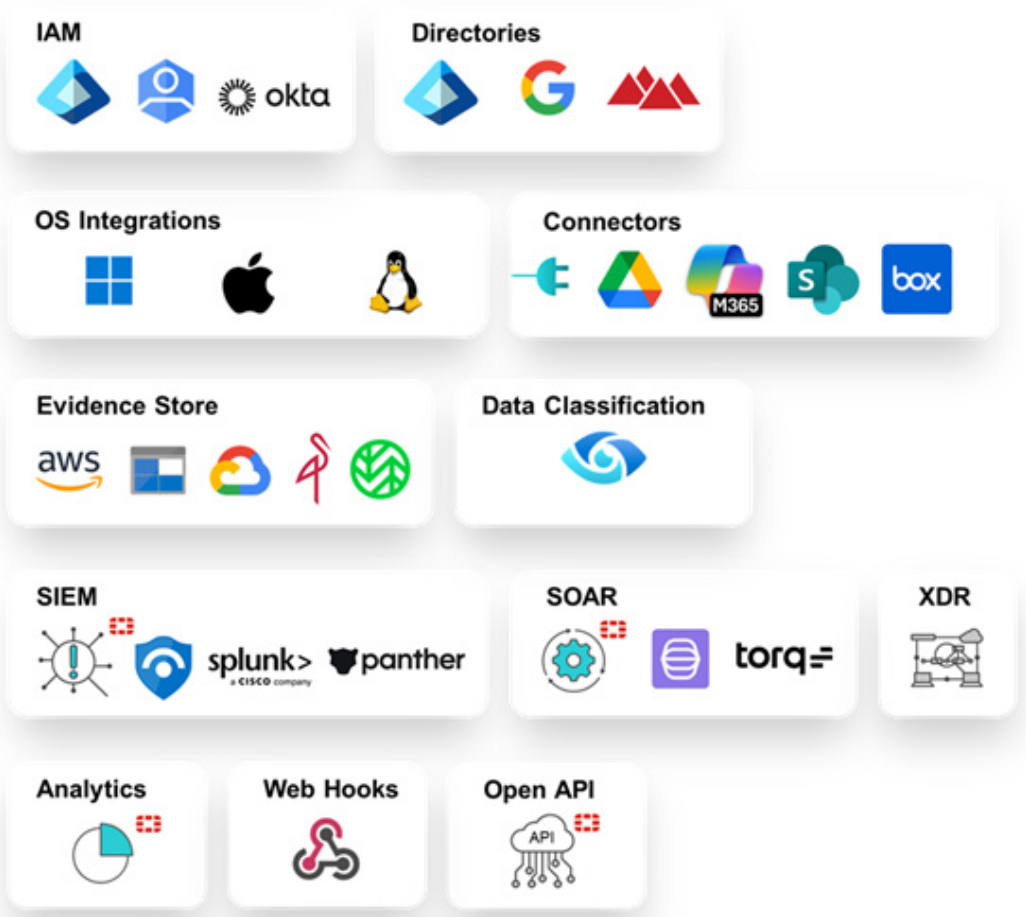
In addition, FortiDLP utilizes FortiAI (AI Assistant) to contextualize data and summarize activities associated with high-risk activity, accelerating incident analysis. Activities are mapped to MITRE ENGENUITY™ Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base.

Highlights

- Integrates Data Loss Prevention, Insider Risk Management, GenAI and SaaS Data Security, and Risk-Informed User Education—at the point of engagement with sensitive data—in a single solution
- Is cloud-native, allowing organizations to turn on services and gain immediate, policy-free visibility into business data flows and risks in minutes, with access to analytics and detections
- Addresses regulatory compliance controls involving data loss prevention with minimal effort using templated PII/PHI/PCI policies
- Accurately detects Intellectual Property and sensitive data using advanced data classification, data origin, and identity-based data tracking
- Provides data tracking from its source with full visibility into subsequent data manipulation over time through Secure Data Flow and Data Lineage features
- Automatically sequences high-risk insider threat activity and generates a risk-scored incident to prioritize data exfiltration activity for investigation and case management
- Monitors Gen AI and SaaS application usage, including corporate and personal credentials use
- Supports sensitivity labels from Microsoft, Google Workspace, and other tools

Integrations

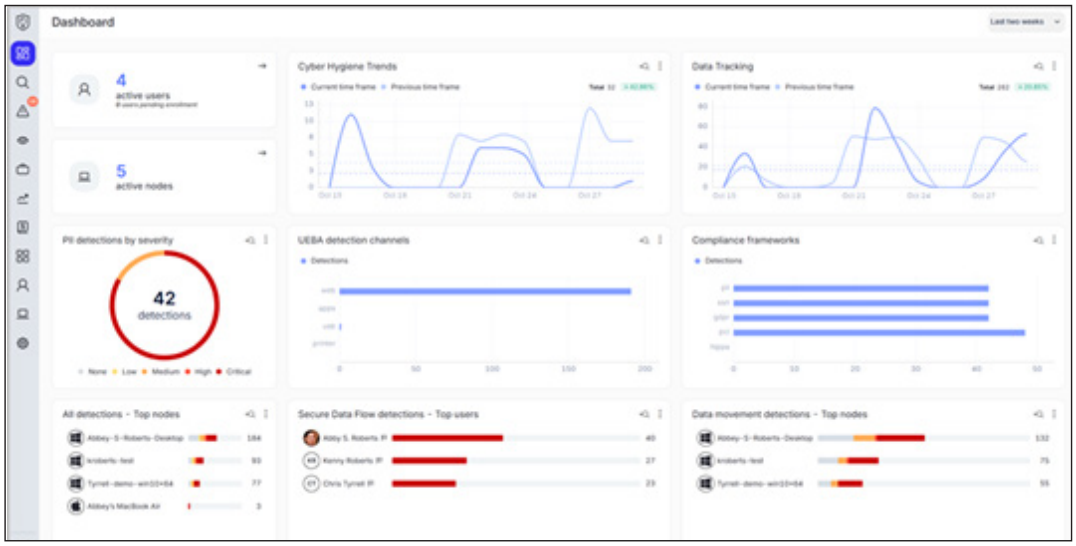
FortiDLP integrates with a growing number of third-party applications and tools, including other solutions across the Fortinet Security Fabric.



Use Cases

Data Loss Prevention

FortiDLP provides rich out-of-the-box data visibility and data protection policies to protect critical information assets on and off the network. FortiDLP analyzes what and how data is being used, and allows you to prescribe policy actions for automatically responding to violations.



Whether your business or other organization relies on structured or unstructured data, FortiDLP can track, and take active steps to prevent its exfiltration or inadvertent disclosure.

FortiDLP agents collect, enrich, and index activity. This data can then be used to:

- Highlight and report on data movement and exposure risk
- Create appropriate data protection policies
- Provide analysts with a rich activity data set to support investigations

Unlike legacy DLP static policies and binary “block” OR “allow” actions, the FortiDLP risk-adaptive policies let you decide which actions to take, such as notifying users via Microsoft Teams or Slack, capturing file and clipboard artifacts, isolating or locking an endpoint, killing a process, or blocking high-risk activity. In addition, features like Secure Data Flow and Data Lineage allow you to prioritize certain data sources and track all interactions and manipulations of data from these sources.

Addresses Key Compliance Controls Involving Data Security and Awareness

FortiDLP enables teams to adopt a proactive stance in meeting key compliance requirements, including PCI DSS, HIPAA, ISO 27001, NIST, and others, to prevent the egress of sensitive data by providing deep visibility into user activities, data access, and systems. In addition, FortiDLP raises awareness of security hygiene through user education at the point of data access.

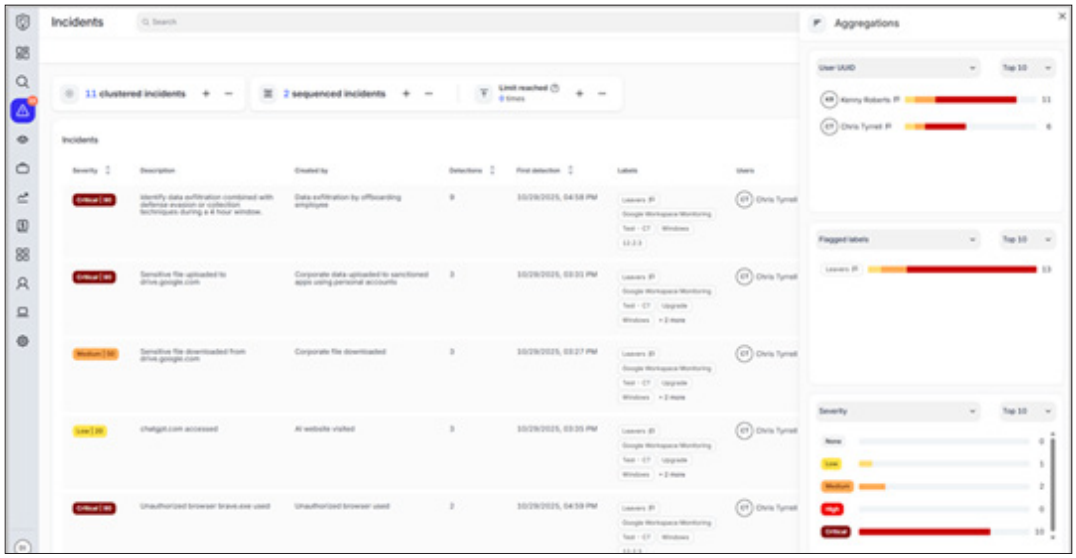
Data Minimization Practices for Privacy of Employee Data

Prioritizing privacy, especially under regulations like GDPR and CCPA, FortiDLP leverages built-in data minimization techniques—such as pseudonymization and localized forensics storage—to help security teams detect and mitigate threats while safeguarding employee confidentiality.

Use Cases Continued

Insider Risk Management

FortiDLP tracks and traces sensitive information flows and user interactions within the organization. It identifies and mitigates insider threats through advanced user behavior analytics, automatically blocking suspicious activities or taking other prescribed action Depending on the severity of the risk, Security Analysts can prompt an employee with an on-screen message, take a screenshot of a user's computer screen, kill a process, kill and block connections to a device, or lock a device.



The FortiDLP activity feed provides analysts with a comprehensive, streamlined, and time-sequenced view of user, data, and device activity before, after, and during an incident. High-risk activity detections are mapped to MITRE Center for Threat-Informed Defense Insider Threat TTP Knowledge Base and automatically sequenced into risk-scored incidents through our Sequence Detection feature.

Depending on the severity of the risk, Security Analysts can prompt an employee with an on-screen message (AKA "nudge" communication), take a screenshot of a user's computer screen, kill a process, kill and block connections to a device, or lock a device.

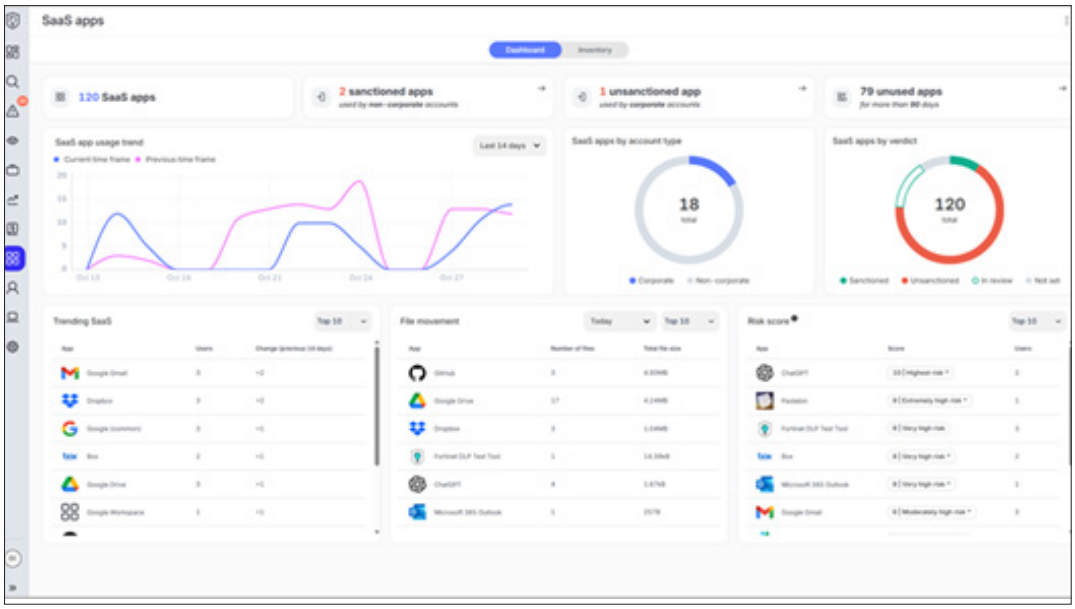
Integrated case management allows analysts to create cases for documenting incidents and associated events, detections, and forensics artifacts as part of the investigation. FortiDLP case management is integrated with FortiAI for automated contextualization and summarization of activities, significantly reducing the time required for analysts to conduct and document their investigations.

Use Cases continued

GenAI and SaaS Data Security

FortiDLP provides comprehensive visibility into user interactions with data in the cloud and maintains protection as data moves out of the cloud. This feature ensures continuous protection of sensitive information, regardless of its location or access method.

The solution builds a comprehensive risk-scored inventory of SaaS applications and GenAI tools utilized across an organization, with insights into data ingress, egress, and credentials. It also fortifies defenses against potential data breaches stemming from business data exposure via unauthorized app usage, nudging employees to use only authorized SaaS applications including sanctioned GenAI tools.



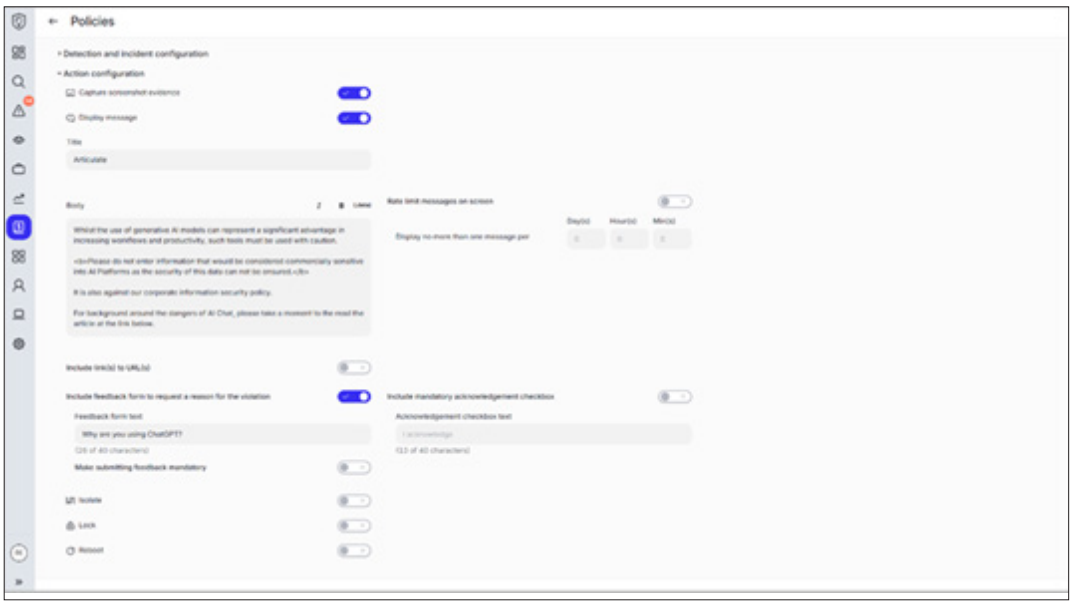
Shadow AI

FortiDLP enables the safe use by employees of publicly available generative-AI tools such as OpenAI ChatGPT, Google Gemini, and other AI tools. Administrators can set policy actions to alert on proper data handling practices while allowing employees to continue using these tools. The result is a balance between enabling productivity while securing the organization against the sharing of sensitive data, either through file uploads or the pasting of content, with these tools.

Use Cases continued

Risk-Informed User Education in Real Time

FortiDLP champions being proactive in risk mitigation, making employees part of the organization's security posture and enabling a more aware and accountable security culture. Customized prompts and nudge notifications—delivered at the point of access and manipulation of sensitive data—reinforce security policy awareness and can direct users to acceptable alternatives when unauthorized apps are detected. Notifications can be sent via endpoint dialogue, email, Microsoft Teams, and Slack messaging systems.



FortiDLP provides constant enforcement without exception—whether employees are remote or working offline. Enforcing employee adherence to corporate policies such as Acceptable Use Policy (AUP), Information Security Policy (ISP), and more.

Key Features - what sets FortiDLP apart

Next-gen Data Loss Prevention and Insider Risk Management

Developed as a direct response to the challenges associated with traditional data loss prevention solutions, FortiDLP delivers comprehensive visibility into user interactions with sensitive data and insider risks, with powerful tools to help you detect, respond to, and prevent data theft and loss.

Scalable, Lightweight Agent—Minimize the Impact of Processes

The FortiDLP agent inspects content and data in movement, lowering the CPU and memory impact on your employees' computers. As a cloud-native solution, FortiDLP scales to your organization's needs regardless of size.

Context and Content Analysis—Perform Real-time Inspection

FortiDLP applies machine learning embedded in each endpoint agent for individual user baselining coupled with contextualized analysis and real-time content-level inspection (at the time of access) to determine if data is sensitive, how it needs to be protected, and perform automated actions per policies.

Expansive Policy Actions—Take Action That Best Suits Circumstances

Unlike legacy DLP binary "block" or "allow" policy actions, with FortiDLP you can respond as your business demands. FortiDLP adaptive controls let you decide what actions to take such as logging, delivering a nudge communication to users, requiring a user acknowledgment, blocking an action, performing a screen capture, creating a file copy. or isolating and even locking an endpoint.

Insider Risk Sequence Detection—Sequence High-Risk Attack Campaigns

FortiDLP automatically identifies, sequences, and scores high-risk activity chains. This capability enables analysts to prioritize their investigation time and move away from manually reviewing thousands of atomic "DLP incidents."

Detections are also automatically mapped using MITRE Center for Threat-Informed Defense Insider Threat TTP Knowledge Base.

Secure Data Flow and Data Lineage—Track Data Movement From its Origin

Secure Data Flow raises the bar on data protection by addressing the limitations of traditional DLP solutions. By tracking the "What, Where, Who, and How" of data origin, movements, and modifications, Secure Data Flow and Data Lineage give analysts performing an investigation the full history of data journey.

Secure Data Flow automatically identifies and tracks data based on its origin. DLP and insider risk policies can be enforced whether a corporate or non-corporate account was used to egress data.

AI Powered Assistant—Accelerate Security Operations and Incident Response

FortiDLP is integrated with FortiAI to enhance incident analysis by summarizing and contextualizing data associated with observed high-risk activity, mapped to MITRE Center for Threat-Informed Defense Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base, for easy consumption by analysts and peers. Analysts benefit from optimized workflows, reducing the time to contain and resolve threats, and the empowerment to contribute to the business at a higher level.

Feature Matrix

FEATURES	STANDARD	ENTERPRISE	MANAGED
DLP			
Device Control	✓	✓	✓
GenAI and SaaS Application Inventory with Data Risk Analytics	✓	✓	✓
Inline DLP for Web, Email, Printers, Clipboard and Removable Media	✓	✓	✓
Real-time Content Inspection (On and Off Network)	✓	✓	✓
Secure Data Flow: Data Loss Prevention Based on Data Origin	✓	✓	✓
Data Lineage Tracking with File Manipulation Detection	✓	✓	✓
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 Management			
Visibility into User Activity Across Endpoints and Enterprise Cloud Drives		✓	✓
Machine Learning-Powered Behavior Analytics		✓	✓
MITRE ATT&CK®-mapped Insider Threat Detection Library		✓	✓
Insider Threat Data Exfiltration Sequence Detection		✓	✓
Endpoint Isolate and Lock Actions		✓	✓
Evidence Store Support for Screen Capture Forensics		✓	✓
Case Management		✓	✓
Enterprise SaaS 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			✓

Ordering Information

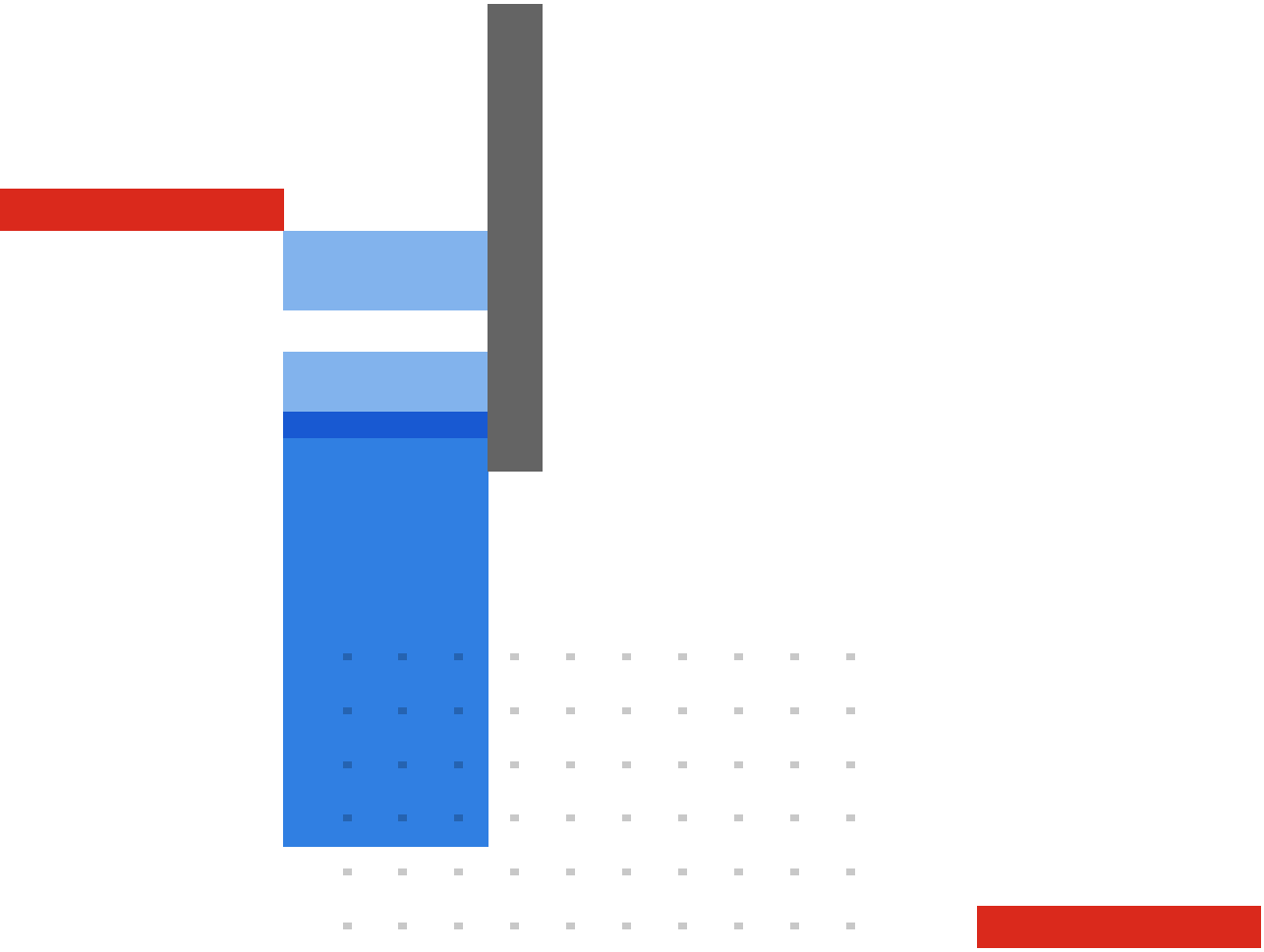
SOLUTION	DESCRIPTION	NUMBER OF ENDPOINTS	SKU	MOQ
SUBSCRIPTION LICENSES				
FortiDLP Core	Endpoint DLP, Secure Data Flow with Data Lineage and FortiCare Premium	100-499	FC2-10-DLPEP-1097-02-DD	100
		500-1999	FC3-10-DLPEP-1097-02-DD	
		2000-9999	FC4-10-DLPEP-1097-02-DD	
		10 000+	FC5-10-DLPEP-1097-02-DD	
Enterprise-Endpoint DLP with Insider Risk and cloud drive integration	Cloud-native endpoint DLP, Insider Risk, and SaaS integration with FortiCare Premium	100-499	FC2-10-DLPEP-1098-02-DD	
		500-1999	FC3-10-DLPEP-1098-02-DD	
		2000-9999	FC4-10-DLPEP-1098-02-DD	
		10 000+	FC5-10-DLPEP-1098-02-DD	
MANAGED SERVICE				
Managed-Enterprise DLP license with managed service	Managed cloud-native Enterprise DLP, Insider Risk, and SaaS integration with FortiCare Premium	100-499	FC2-10-DLPEP-1099-02-DD	100
		500-1999	FC3-10-DLPEP-1099-02-DD	
		2000-9999	FC4-10-DLPEP-1099-02-DD	
		10 000+	FC5-10-DLPEP-1099-02-DD	
FORTICARE BEST PRACTICES CONSULTATION SERVICE				
Forticare Best Practices Consultation Service (BPS)*	Number of endpoints/users	Up to 999	FC1-10-DLBPS-310-02-DD	—
		1000-9999	FC2-10-DLBPS-310-02-DD	
		10 000+	FC3-10-DLBPS-310-02-DD	
ENTERPRISE PREMIUM SERVICE				
Enterprise - Endpoint DLP with Insider Risk and cloud drive integration	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	
		10 000+	FC5-10-DLPEP-1098-02-DD	
Enterprise Premium - Endpoint DLP with Risk and cloud drive integration on premium PoP	Cloud-native Endpoint DLP, Insider Risk and SaaS integration on premium PoP location with FortiCare Premium	100-499	FC2-10-DLPEP-1174-02-DD	
		500-1999	FC3-10-DLPEP-1174-02-DD	
		2000-9999	FC4-10-DLPEP-1174-02-DD	
		10 000+	FC5-10-DLPEP-1174-02-DD	

* BPS required.

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

Copyright © 2025 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.

October 29, 2025

FDLP-DAT-R05-20251029