SOLUTION BRIEF

Prevent Data Loss with Fortinet FortiDLP

Executive Summary

Securing data is more challenging than ever because of the complexity of today's IT environments, new sensitive data regulations, and an explosion of data related to digital intellectual property, hybrid working and return-to-office mandates, as well as personal employee apps and shadow AI usage. Unfortunately, existing data protection programs and traditional legacy DLP tools have failed to mitigate risk and protect data. Preventing data loss now requires a modern cross-platform approach.

FortiDLP is a next-generation, AI-enhanced, cloud-native data protection solution that helps security teams 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. FortiDLP helps prevent data loss, provides immediate visibility into data, derives insights into business data flows, drives prioritized investigations, and detects high-risk activity across users, endpoints, and cloud drives, and enables prioritized investigations.

By 2027, 70% of organizations will combine DLP and insider risk management disciplines with IAM context to identify suspicious behavior more effectively.[1]

Keeping Data Safe Can Be Challenging

Even though many organizations have DLP programs and solutions, CISOs and security leaders are once again asking their teams how to keep data safe without adversely impacting business operations or slowing down productivity. Organizations need a solution that:

- Prevents unauthorized transfer of sensitive data outside the organization, whether through email, cloud storage, physical devices, or other points of egress
- Identifies and mitigates risks posed by malicious insiders who may have access to sensitive data
- Addresses the use of authorized and unauthorized cloud applications and services, which can increase the risk of data breaches
- Enables employees to safely use publicly available generative AI tools such as OpenAI ChatGPT and Google Gemini
- Simplifies the deployment and management of DLP solutions, eliminating the need for extensive IT infrastructure and prebuilt policies

A Unified Approach to Data Protection

FortiDLP applies a modern and unified approach to data protection, combining DLP, insider risk management, SaaS data security, behavioral analytics, and risk-informed user education. Unlike traditional approaches, FortiDLP doesn't require IT infrastructure, exhaustive data discovery and classification, or prebuilt policies.

The cloud-native design of FortiDLP means it can be deployed in minutes through a powerful agent and connectors to provide visibility into business data flows and data protection starting on day one. The lightweight, scalable agent technology in FortiDLP inspects content and data in motion. Once the agent and SaaS connectors are deployed, FortiDLP sees the interactions between users, teams, and data without requiring discovery, labeling, or policies.

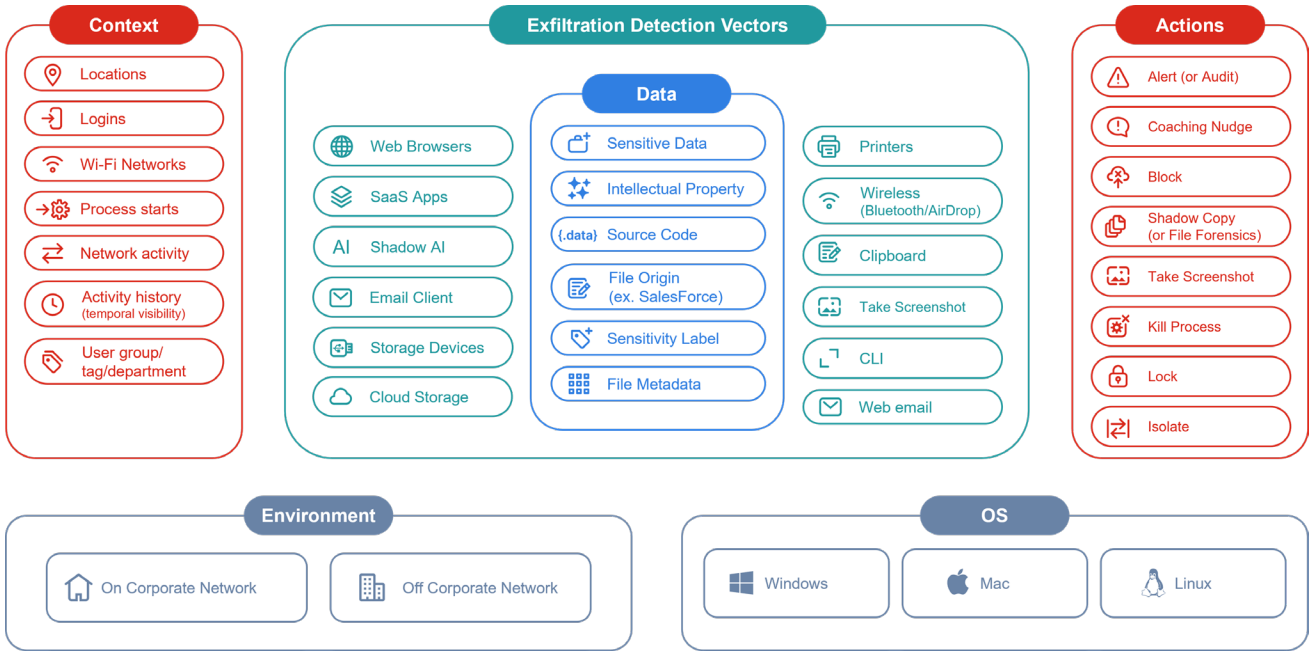

Figure 1: How FortiDLP works

FortiDLP uses machine learning integrated into its agent to baseline activity. It then uses behavioral analytics algorithms and context and content-level inspection to detect typical versus novel or anomalous behavior. Using this information, incident analysts can prioritize investigations into observed high-risk or suspicious activity.

FortiDLP has an AI assistant that summarizes and contextualizes data associated with high-risk activity to accelerate incident analysis with activities mapped to MITRE Engenuity™ Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base. Because FortiDLP is cloud-native, organizations can turn on services and gain data risk visibility in minutes to protect sensitive data. It also:

Data is under threat more than ever. The average cost of a data breach is now $4.88 million in 2024, up 10% from 2023.[2]

- Monitors SaaS application usage, including shadow AI tools like GenAI, while incorporating risk-informed user education at the point of access to sensitive data
- Provides an up-to-date management console and behavior analytics system to monitor, report, and enable automated actions
- Delivers immediate policy-free visibility into data movement
- Accurately detects intellectual property and sensitive data using advanced data classification, data origin, and identity-based data tracking
- Addresses regulatory compliance controls involving data loss prevention with minimal effort using templated PII/PHI/PCI policies

Next-Gen Data Loss Prevention

FortiDLP provides rich data visibility, risk assessment, 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 determine how to best respond. FortiDLP:

- Prevents data loss from exfiltration and accidental loss
- Monitors for insider threats and high-risk employees
- Secures data in use by SaaS and other applications
- Applies user and entity behavioral analysis at scale

- Educates users on proper data handling at the point of access of sensitive data
- Identifies shadow AI usage and stops the upload of sensitive data

FortiDLP doesn't require prebuilt policies. It classifies and tracks data in real time for immediate visibility and data protection. Whether an organization relies on structured or unstructured data, FortiDLP can track and take active steps to protect it.

FortiDLP automatically collects, enriches, and indexes activity across event types, such as authentication, web, email, applications, USB, file creation, sharing, and download activity. This data set is then used to:

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

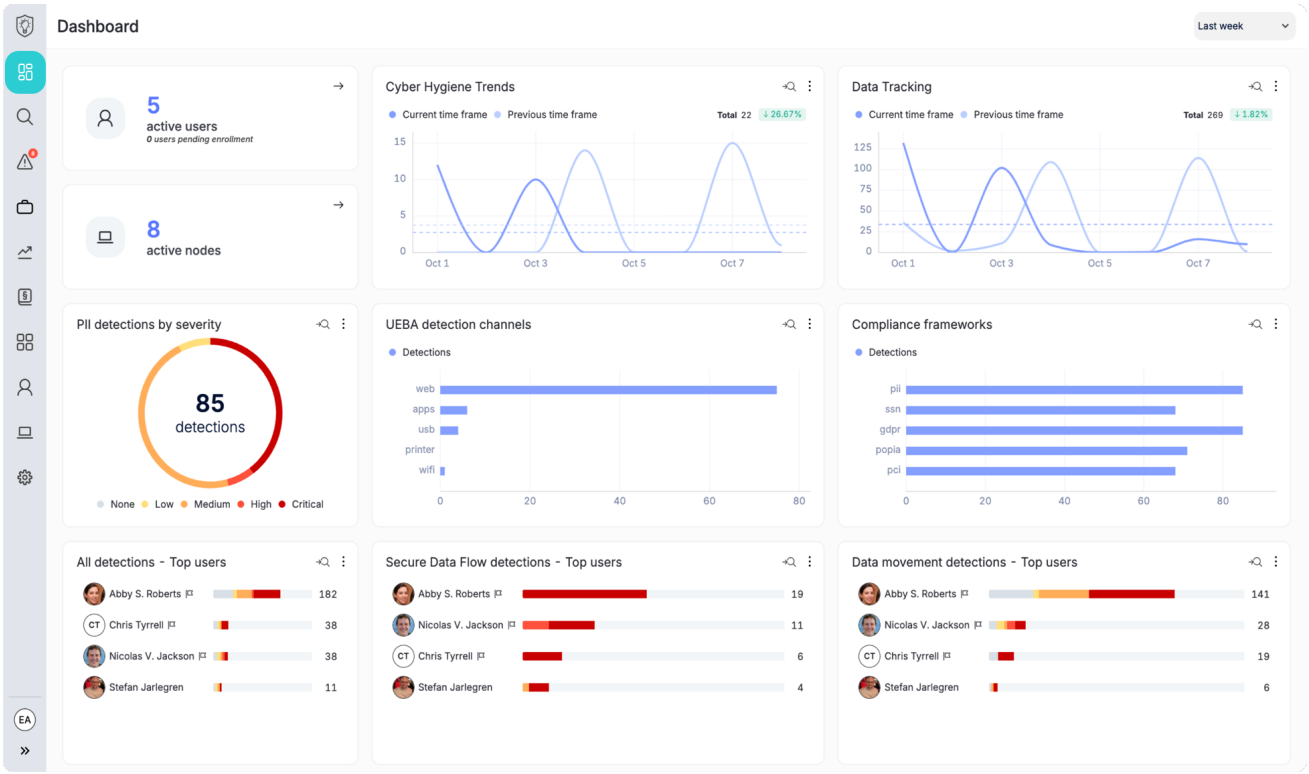

Figure 2: FortiDLP view into data flows and potential risks

Insider risk

The FortiDLP activity feed provides 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 the MITRE ATT&CK framework and automatically sequenced into risk-scored incidents to help analysts prioritize investigations.

Secure data flow

Secure data flow tracks and traces file movement across managed endpoints and cloud applications to protect data based on its origin. The full history of the data's journey, including where it originated, where it's been, who handled it, and what it did, are mapped to the MITRE Insider Threat Knowledge Base, accelerating security operations and incident response.

Risk-informed user education

Risk-informed training trains employees to make the right decisions based on detection of unacceptable behavior. It reinforces corporate security policies and promotes good cyber hygiene.

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 visibility into interactions helps ensure continuous protection of sensitive information, regardless of its location or access method.

Shadow AI

Administrators can set policies to address shadow AI usage that strikes a balance between enabling greater productivity while alerting employees against the sharing of sensitive data.

Safeguard Data and Mitigate Risks

Organizations face unprecedented challenges in protecting their sensitive data. Traditional data loss prevention approaches have proven ineffective with the rise of remote work, cloud adoption, and the proliferation of unmanaged devices. FortiDLP, a next-generation cloud-native endpoint DLP solution, offers a comprehensive solution to meet these challenges, providing the tools organizations need to safeguard their data and mitigate risks.

[1] Gartner, Gartner Unveils Top Eight Cybersecurity Predictions for 2024, March 18, 2024.

[2] IBM and Ponemon Institute, Cost of a Data Breach Report 2024, July 30, 2024.

October 30, 2024 12:50 AM / MKTG-185-0-0-EN