SOLUTION BRIEF

Deliver Real-Time Protection Against Data Exfiltration, Insider Threats, and Shadow AI with the FortiGuard DLP Service

Executive Summary

In an era of hybrid work and rapid AI tool adoption, sensitive data is no longer confined within a corporate perimeter. As organizations shift toward data-centric security, they face an uphill battle against shadow AI, data breaches, insider threats, and sophisticated data exfiltration tactics across files, applications (including GenAI), and images. In addition, global privacy regulations are becoming increasingly stringent and punitive, with governance and compliance being mandatory requirements.

The FortiGuard Data Loss Prevention (DLP) Service provides a frictionless approach to data security. Integrated directly into the Fortinet Security Fabric, it offers real-time visibility and control over sensitive information in motion. Whether the threat is a malicious cyberattack seeking to exfiltrate code or a negligent employee accidentally sharing documents, FortiGuard DLP ensures that proprietary intelligence and regulated information remain secure without the complexity of traditional, siloed products.



15% of employees routinely accessed GenAI tools on their corporate devices, with 72% of those users signing in using personal email accounts and 17% using corporate emails without authentication systems.[1]

Data Security Challenges of the Modern Enterprise

Today's organizations must secure fragmented data across multiple environments while cyberattacks increase in sophistication and speed. Security teams must contend with:

- **A lack of traditional perimeter:** With the rise of remote work and cloud computing, data no longer sits behind a physical firewall. It is constantly in motion across public networks and unmanaged home environments.
- **The shadow AI explosion:** The democratization of GenAI tools has created a massive, unregulated outflow point. Employees frequently input sensitive code, legal documents, and strategy papers into public large language models (LLMs), leading to permanent data exposure and compliance issues.

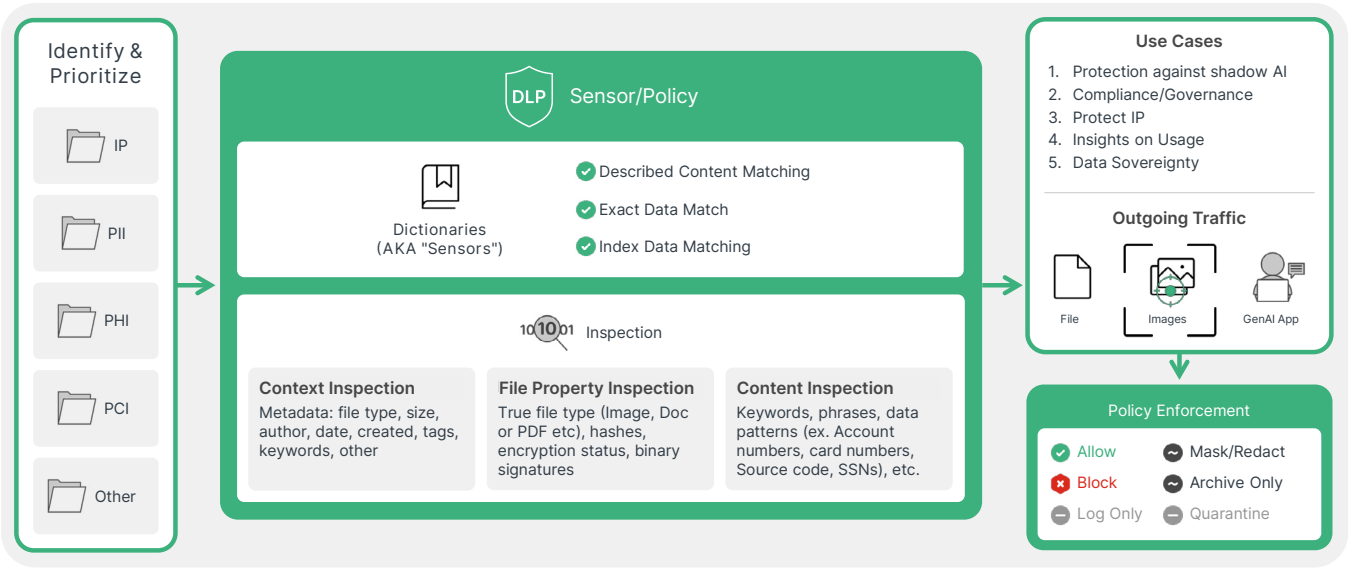


Figure 1: FortiGuard DLP Service overview

- **A large volume of unstructured data:** The majority of enterprise data (80%) is unstructured (images, chat logs, video),[2] which is not easy to identify. This creates a massive "dark data" blind spot that hides sensitive information from oversight, making it difficult for traditional security controls to detect issues.
- **Sophisticated exfiltration:** Modern threats are no longer simple file transfers. Data is now leaked through analog hole tactics like scanning and screen captures or malicious code injection designed to bypass standard threshold alerts. This leads to financial and reputational losses, and in some cases, violations of data sovereignty laws.

Key Capabilities and Detection Techniques

The service utilizes a multilayered detection engine to provide granular visibility and control across diverse data categories.

Predefined data templates offer instant, out-of-the-box protection categorized by:

- **Government and identity records:** Comprehensive support for global identification, including driver's licenses (various countries, U.S. states, and Canadian provinces), and national tax IDs (SSN, ITIN, SIN)
- **Financial intelligence:** Automated detection of credit card numbers, SWIFT codes, and complex financial records
- **Regulated privacy data:** Pre-mapped templates for personally identifiable information (PII) and protected health information (PHI) to ensure continuous compliance with GDPR, HIPAA, and local privacy laws
- **Corporate intellectual property (IP):** Specialized patterns to identify and shield proprietary designs, source code, and strategic business documents

Advanced matching engines allow the service to move beyond simple word searches and understand the context and uniqueness of the data so it can tell the difference between sensitive and non-sensitive data.

- **Described content matching:** Using proximity search and confidence levels to identify sensitive data
- **Exact data matching:** Fingerprinting specific database records for zero-leak precision
- **Index and dictionary matching:** Tracking custom, industry-specific, or proprietary terminology

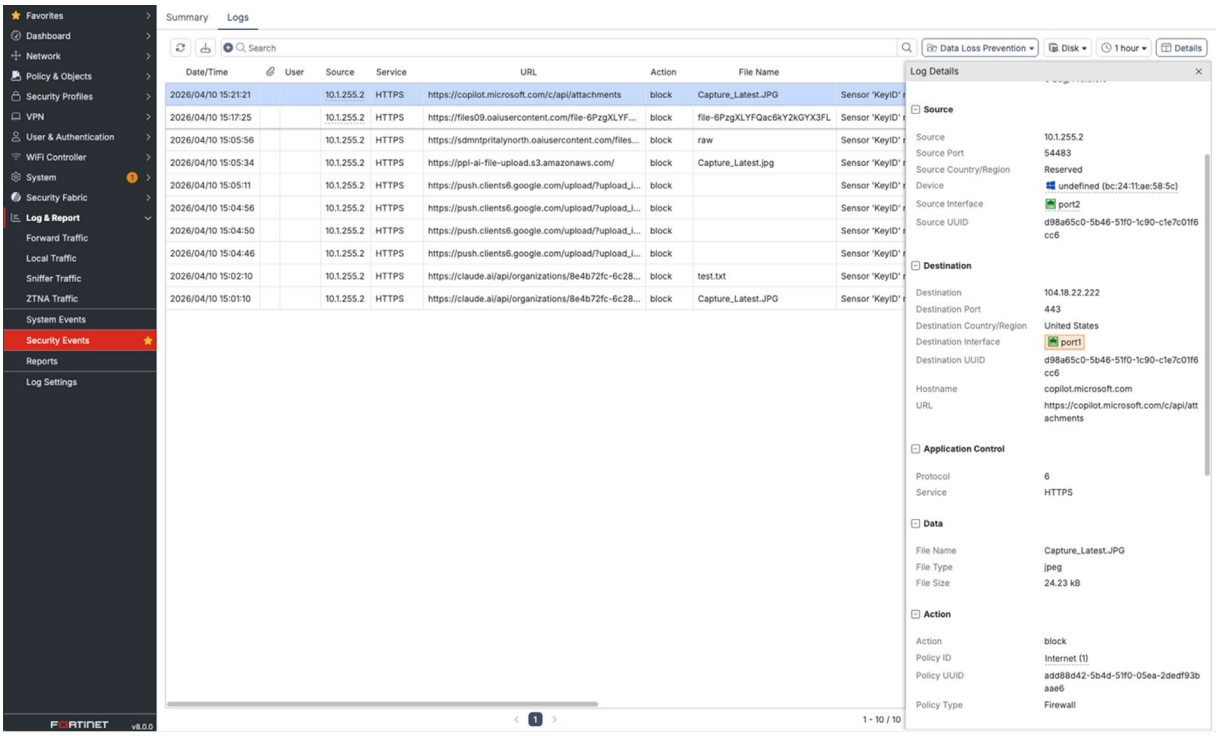


Figure 2: FortiGuard DLP Service in action

Multidimensional data inspection distinguishes legitimate business workflows from potential exfiltration. FortiGuard DLP employs AI-powered inspection across three dimensions:

1. **Content inspection** provides deep-packet analysis to identify sensitive data within the payload. It uses AI-enhanced patterns to detect complex strings like SSNs and financial data alongside AI linguistic analysis to protect proprietary source code.
2. **File property inspection** analyzes the file's DNA to defeat evasion. It uses true file type ID and binary signatures to identify the actual format (PDF, image), preventing users from bypassing security by simply changing a file extension.
3. **Context inspection** evaluates metadata and environmental factors. It correlates metadata analysis (size, author, tags) with AI behavioral context to identify anomalous intent, such as an author uploading sensitive project files to a personal GenAI app.

Optical character recognition (OCR) extracts text from images, scans, and screenshots to ensure visual media is governed by the same strict policies as text files.

- **Closes the screenshot security gap** by scanning standalone images (JPG, PNG, GIF) to check against DLP policies, preventing users from bypassing "no copy/paste" rules by simply taking a picture of their screen
- **Gives visibility into hidden data** with deep content inspection to find embedded images within complex files (like a ZIP or a Word doc) and extract text to find sensitive identifiers
- **Defeats analog hole attacks** by reconstructing digital text from scanned documents to ensure the data's sensitivity is recognized and malicious insiders are not able to strip away metadata via printing and scanning a document
- **Ensures regulatory compliance** by enabling FortiGuard DLP to apply predefined templates to visual media, ensuring a scanned ID or photo of a credit card triggers the same protections as a spreadsheet would have
- **Protects against image-based phishing** by reading text inside images (like fake login prompts) and blocking threats before they reach the user

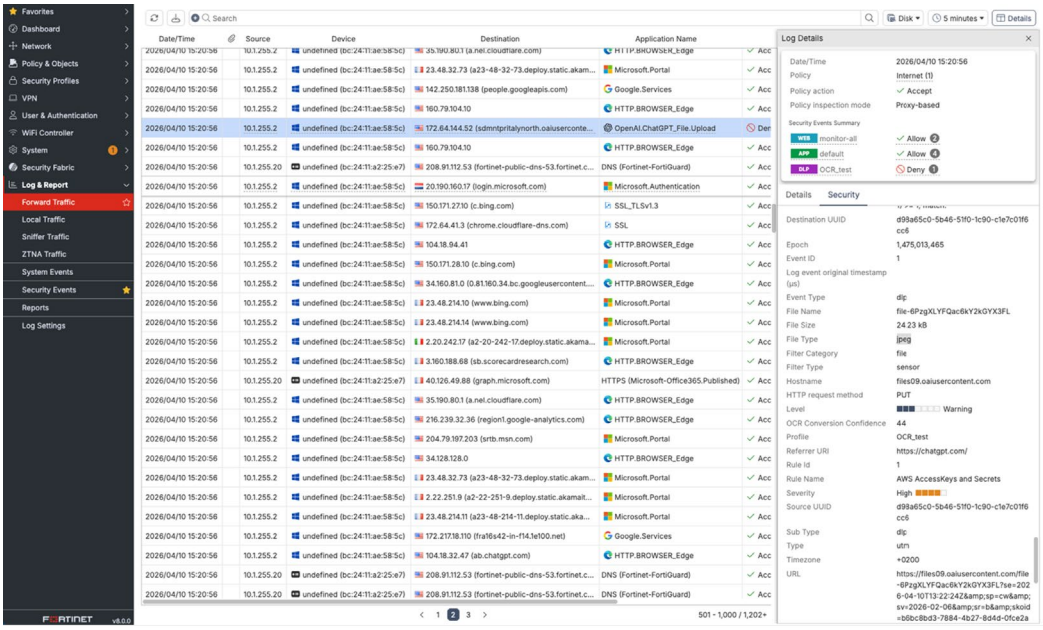


Figure 3: FortiGuard DLP Service OCR scanning and protection

FortiGuard DLP Integration with Fortinet Security Fabric Platform Solutions

One key advantage of our platform-driven approach is fast, automated, and coordinated response to threats across the entire enterprise infrastructure. The FortiGuard DLP Service can integrate into:

- **FortiGate Next-Generation Firewalls** for high-speed network inspection and enforcement
- **Fortinet Secure SD-WAN** to secure data across distributed branch architectures

- **FortiSASE** to enable consistent DLP policy for remote and hybrid workers
- **FortiCASB** (API CASB) for governance of data residing in SaaS environments like Office 365 or Salesforce

These integrations allow for Security Fabric orchestration, enforcing a single policy across FortiGate (network), FortiSASE (cloud edge), and FortiCASB (SaaS), closing gaps in the security posture.



The average cost of a malicious insider attack has reached $4.92 million per incident, while breaches involving shadow AI add an average of $670,000 to the total breach price tag.[3]

FortiGuard DLP Service Benefits

Beyond mere technical enforcement, FortiGuard DLP acts as a strategic enabler, providing the governance and security necessary for the enterprise to grow safely in a data-centric world.

Secure AI adoption with protection against shadow AI

Mitigate the risks of unregulated AI tool adoption by preventing unauthorized file uploads and prompt-based interactions. This category is critical for stopping data exfiltration, sensitive data leakage, and unintended exposure resulting from employees using unsanctioned GenAI applications.

Avoid fines and audit failures with automated compliance and governance

Automate the discovery and protection of regulated data categories (PII, PHI, financials) to meet global mandates like GDPR, HIPAA, and PCI-DSS. It ensures that data handling aligns with internal governance policies across the entire Security Fabric.

Maintain competitive advantage with intellectual property protection

Safeguard critical enterprise data, such as proprietary source code, blueprints, and strategic roadmaps. By using exact data matching and document fingerprinting, FortiGuard DLP prevents the unauthorized transfer of IP within files and AI-enhanced applications.

Get insights on usage and threats, including insider threats

Enhance operational resilience with deep visibility into how data is moving across the organization. This telemetry is essential for detecting insider threats, identifying anomalous behavior from compromised accounts, and understanding data flow patterns to improve security posture. This enables the SOC to detect issues in real time.

Simplify operations with data sovereignty enforcement

Maintain strict control over where your data resides and how it is transmitted across borders. This is vital for meeting localized data residency requirements and ensuring that sensitive information does not cross restricted geographic or logical boundaries.

Proactive Data Protection with FortiGuard DLP

The FortiGuard DLP Service transforms data protection from a reactive bottleneck into an intelligent, automated business enabler. By integrating advanced AI, OCR, and broad Security Fabric orchestration, Fortinet provides a future-proof solution that protects the modern enterprise against the data security threats of today and tomorrow.

[1] 2025 Data Breach Investigations Report, Verizon, April 23, 2025. https://www.verizon.com/business/resources/T16f/reports/2025-dbir-data-breach-investigations-report.pdf

[2] Unstructured Data: Unlocking Insights with AI, Datahub Analytics, April 16, 2025. https://datahubanalytics.com/unstructured-data-unlocking-insights-with-ai

[3] Cost of a Data Breach Report 2025: The AI Oversight Gap, IBM, July 30, 2025. https://www.ibm.com/reports/data-breach

FORTINET

www.fortinet.com

Copyright © 2026 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.

April 28, 2026 10:11 AM / MKTG-3284-0-0-EN