proofpoint

SOLUTION BRIEF

Proofpoint Enterprise DLP

Transform your data security program and architecture

Key Benefits

- Prevent data loss across email, cloud, endpoints, and GenAI applications
- Accelerate incident resolution, including DLP alert triage, investigation, and response
- Deploy quickly, scale automatically, and simplify maintenance
- Meet data privacy requirements in the United States and other regions

Today's workers put data at risk in more ways. They use personal devices to access cloud applications and share data across email, endpoints, and collaboration tools. In addition, unapproved generative AI (GenAI) tools are often just a browser click away. Security teams are working harder to protect privacy, maintain compliance, and support responsible GenAI adoption. Breaches now bring growing financial, reputational, and audit consequences.

Organizations need better visibility of sensitive data. They also need to see how users handle it across email, cloud, endpoints, and GenAI apps. However, legacy data loss prevention (DLP) tools are often siloed, hard to scale, and inconsistent across channels. They're also unable to address emerging AI-related risks.

Proofpoint Enterprise DLP drives a unified, adaptive approach to data loss prevention (DLP). It helps stop data loss caused by people across email, cloud, endpoints, and AI apps. It also helps security teams work more efficiently.

Proofpoint identifies sensitive content and shows how employees use it. The unified console helps you manage alerts and investigate incidents across all channels. Analytics and AI classification help teams assess data risk, reach better verdicts, and act fast. The solution runs in the cloud, scales on its own, and is easy to deploy and maintain. It also has modern privacy controls and a highly stable agent.

Reduce Data Security Risk Across Channels

A Clear View of User Behavior

Proofpoint monitors how workers use data across email, managed and unmanaged endpoints, GenAI tools, and cloud apps. These include Microsoft 365, Google Workspace, and Salesforce. It reveals user intent and detects and prevents exfiltration. Examples include copying files to an unauthorized USB drive, uploading sensitive files to a personal cloud folder, or sharing confidential information through AI prompts.

Proofpoint helps organizations securely adopt GenAI. It detects, blocks, and redacts sensitive data before it's shared with sanctioned or unsanctioned AI apps. Teams can enforce policy in browser and desktop AI apps. Intelligent remediation and guided user experiences help users stay productive.

Proofpoint monitors and controls:

- File uploads to AI apps
- Copy-and-paste activity involving sensitive data
- AI prompts with regulated or proprietary information
- Sensitive attachments shared through email and cloud collaboration tools
- Risky user behavior on endpoints and cloud services

Proofpoint integrates with LDAP and Active Directory. You can use groups from these directories to define and dynamically apply detailed email encryption policies. Our solution tracks behaviors such as:

- **File changes**, including renaming files with sensitive data or changing their file extensions
- **Unusual website and application use**, including downloading data backups or hacking tools
- **Dangerous actions by high-risk users**, including manipulating the Windows registry to disable security controls

Accurate Content Identification and AI-Powered Classification

Proofpoint improves detection accuracy with more than 110 ready-to-use AI classifiers. These identify document categories and add business context to DLP alerts. They work with pattern matching, exact data matching (EDM), indexed document matching (IDM), optical character recognition (OCR), and fingerprinting technologies. This combination reduces false positives and improves protection across all channels.

Proofpoint Autonomous Custom Classification (ACC) uses large language models (LLMs) to learn each organization's sensitive content. It does this without manual tuning. Teams can quickly find and protect proprietary data. Examples include source code, financial models, engineering documents, and customer records. This simplifies policy creation and accelerates time to value.

Shared AI-powered detection engines provide consistent protection across enterprise DLP channels. Organizations can detect and classify personally identifiable information (PII), protected health information (PHI), payment card industry (PCI) data, credentials, intellectual property, and confidential business information. LLM-enriched alerts add context so teams can investigate and respond faster.

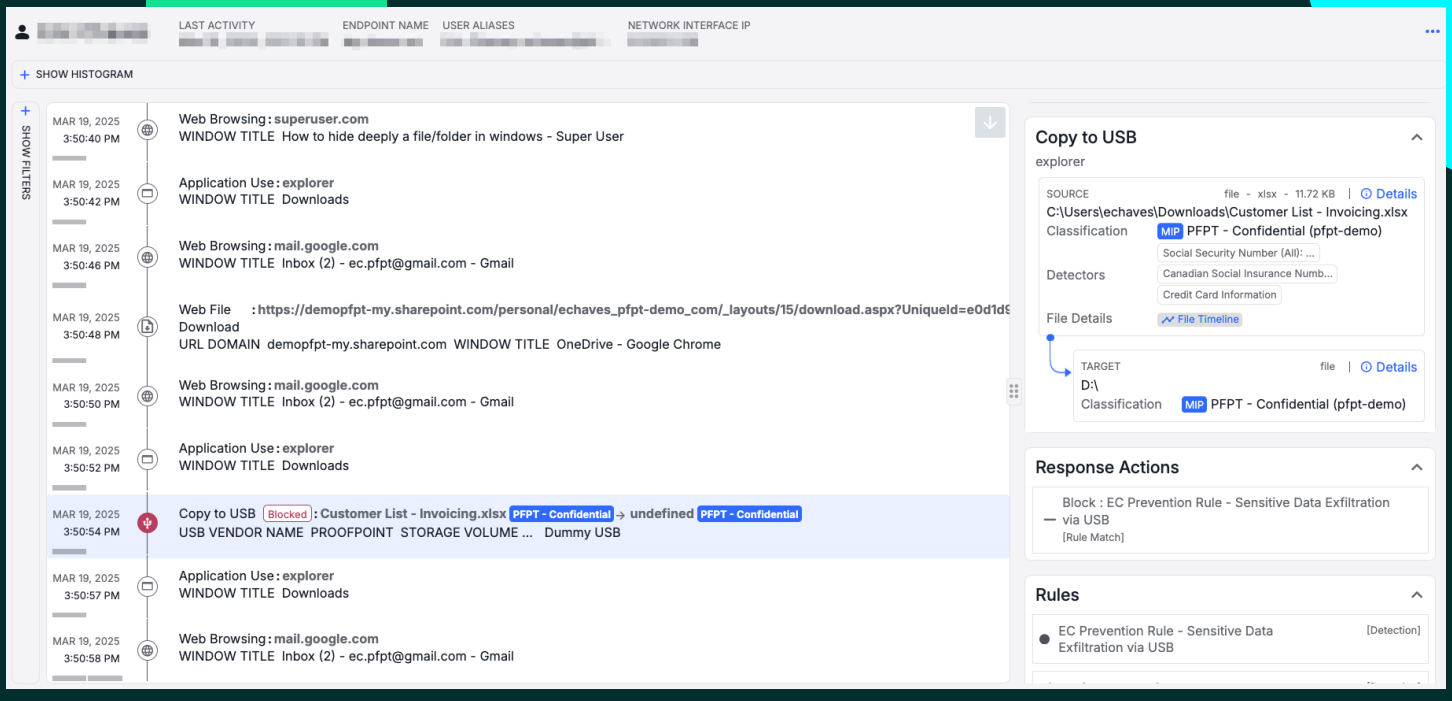

Figure 1: This Data Security Workbench example shows a risky sequence of user actions. The user searches for ways to hide a file, downloads a sensitive file from SharePoint, and tries to copy it to a USB drive. The actions and timeline suggest possible policy evasion that needs further review.

Adaptive Policy Enforcement and Guided User Remediation

Proofpoint provides shared policy enforcement across all DLP channels. Teams can define policies once and apply them consistently.

Adaptive policies help teams monitor high-risk users, understand intent, and automate responses. When an alert appears, these policies collect more metadata and visual evidence. Clearer insights help analysts investigate more quickly and lower total cost of ownership.

Proofpoint also prevents sensitive data loss through GenAI prompts. Our solution guides users toward safer AI use. It automatically fixes broad file sharing in cloud apps. It also asks users to justify copying sensitive data to a cloud folder or to a network drive.

Reduce Operating Costs and Accelerate Incident Resolution

Efficient Cross-Channel DLP Operations

Teams using siloed, legacy DLP tools often face slow investigations, fragmented visibility, and missed policy violations. Proofpoint brings detection, policies, and governance controls together across all DLP channels. Data Security Workbench also centralizes telemetry and alerts. This helps teams triage, investigate, and respond faster.

The Data Security Workbench console provides:

- Timeline views of user interactions with sensitive data (see figure 1)
- Unified alert management and DLP configuration (see figure 2)
- Linked investigations across email, cloud, endpoints, and AI apps
- File lineage tracing as files are created, modified, and shared
- Threat hunting to find and investigate risks earlier
- Dashboards for executives and audit reports

Proactive Data Security

Data Security Workbench lets you search and filter data risks. You can build custom views to manage those risks before they grow. You can search for data exfiltration attempts and other risky activities, such as the use of unapproved GenAI apps. The user timeline shows who did what, where, when, and why.

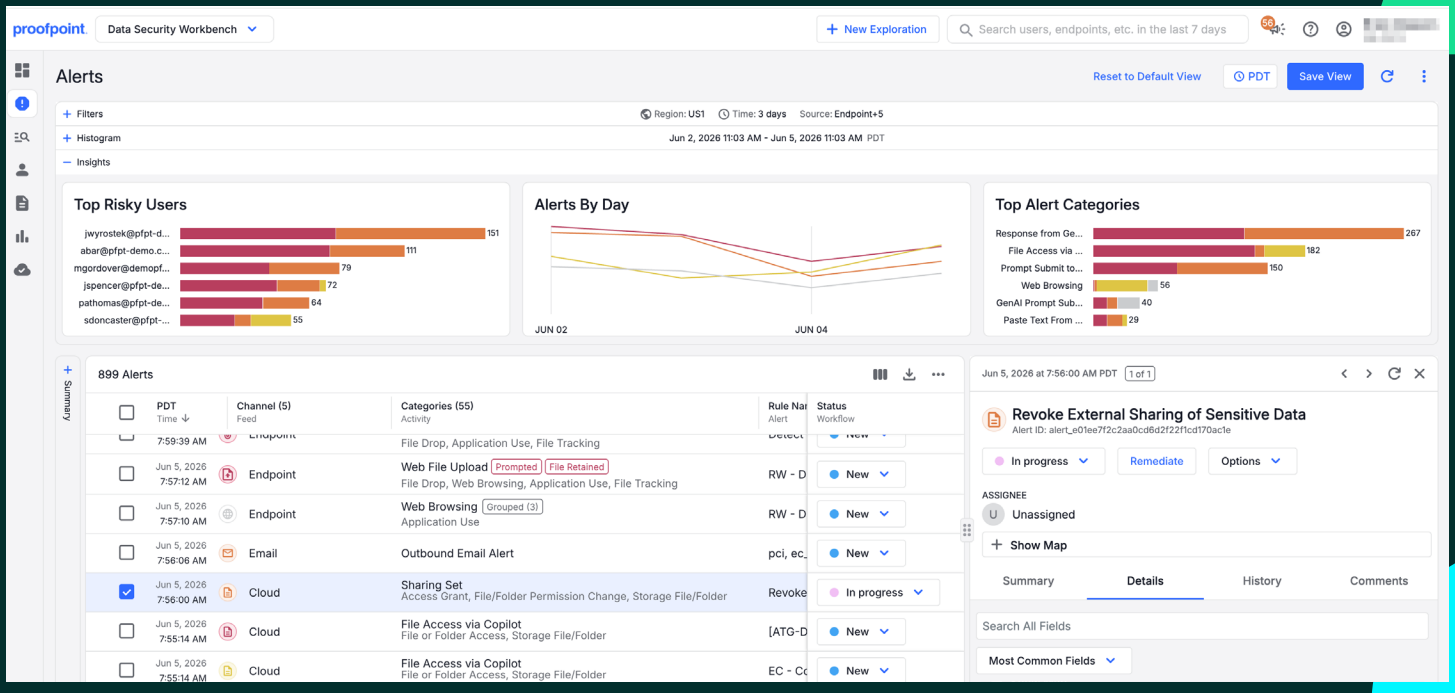

Figure 2: In Data Security Workbench, you can build custom explorations of data risks.

Enable Business Agility with a Modern Architecture

Proofpoint solutions are delivered as services, saving you valuable time. They deploy quickly, scale automatically, and make maintenance easier. They are modular and use shared cloud services. Our cloud-native solutions support multiple tenants and APIs. They are built to scale. They can support hundreds of thousands of users per tenant. The Proofpoint platform integrates with partners such as Microsoft, Okta, Splunk, and ServiceNow.

Granular Data Privacy Controls

Proofpoint provides a global cloud-native console and can store data in multiple regions. Attribute-based access controls limit who can view alerts and investigations by role, function, or region. Data masking and user anonymization (see figure 3) help meet regional privacy and data residency rules.

Highly Stable Endpoint Agent

Our lightweight user-mode agent is stable and quick to deploy. It is unique in how it detects data loss and possible insider threats. You can change the agent's behavior by updating policies in the platform. Unlike kernel-mode agents, the Proofpoint agent provides a reliable user experience. This can reduce help desk tickets and save administrator time.

Shorten Time to Value with Our Expertise

Preventing data loss requires technical and product expertise along with strong data governance skills. Proofpoint applied services help you get more value from your investment, support continuous operations, and mature your data protection program.

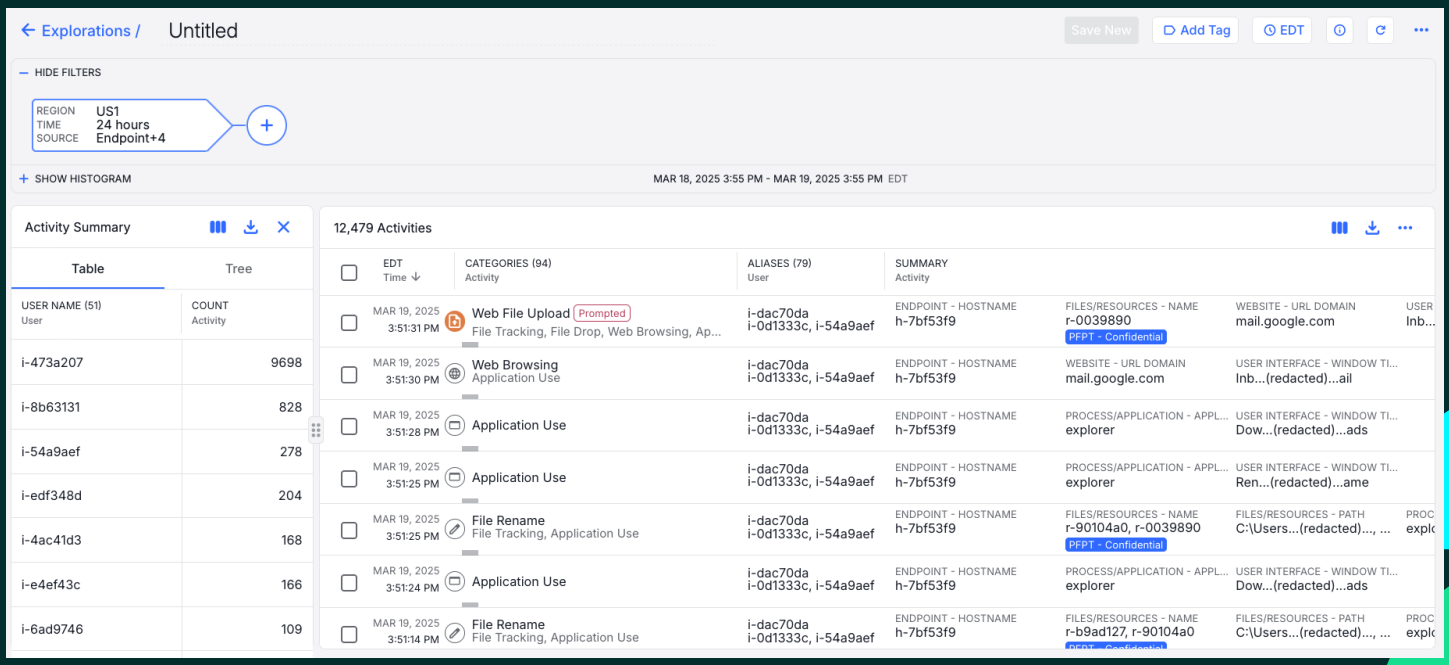

Figure 3: The console can anonymize user details during an investigation. This protects privacy and helps reduce analyst bias.

Key features & capabilities	DLP Transform Tier 1	DLP Transform Tier 2	Add-ons
Deep user and file context	✓	✓	
Threat hunting to detect and investigate sooner	✓	✓	
Single user-mode agent for insider threats and DLP	✓	✓	
Rich DLP detectors (Regex, OCR, IDM, EDM) and MIP classification	✓	✓	
Out-of-the-box AI and autonomous AI classifiers	✓	✓	
Data lineage to monitor and detect file movements	✓	✓	
API, forward, and reverse proxy modalities	✓	✓	
Broad cloud application detectors	✓	✓	
Unified alert management and DLP configuration	✓	✓	
Granular data privacy and access controls	✓	✓	
Security ecosystem integration (SIEM, SOAR, Teams)	✓	✓	
Detection and analysis of sensitive data in email messages and attachments		✓	
Dynamic encryption of external or internal-to-internal email		✓	
Sensitive document fingerprinting in email		✓	
AI-powered prevention of accidental and intentional data loss via email		✓	✓
Discovery and classification of data stores		✓	✓
Exposure risk detection and remediation in data stores		✓	✓
Insider threat visual capture			✓

Learn More

For more information, visit **proofpoint.com**