proofpoint.

SOLUTION BRIEF

Proofpoint Data Loss Prevention

Transform your data security program and architecture.

Key benefits

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

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

Today's workers are putting data at risk in more and more ways. They increasingly use unapproved productivity tools such as generative AI (GenAI). They also use personal devices to access their organizations' cloud applications. Data security teams are finding it harder to keep up, as they are asked to do more with less to ensure data privacy. At the same time, the business consequences of data breaches are becoming more costly. Negative outcomes include financial loss, reputational damage and failed regulatory compliance. Organizations need better visibility of their email, cloud and endpoint data and the behavior of their users. However, legacy data loss prevention (DLP) tools do not meet these needs. Worse, they are often siloed, costly, hard to maintain and difficult to scale.

With Proofpoint's Data Loss Prevention (DLP) solutions, you can transform your data security program and architecture. Our solutions drive an adaptive approach to DLP. As a result, you can address human-driven data loss in your email, cloud, and endpoint channels more effectively and efficiently.

Proofpoint accurately identifies sensitive content and provides deep visibility of user behavior. A single, unified console helps you manage alerts and investigate incidents across all channels. Using powerful analytics, you can quickly assess data risk, reach high-fidelity verdicts and take appropriate actions. Our solutions are built on a cloud-native architecture with modern privacy controls and a highly stable agent. They scale automatically and are easy to deploy and maintain.

Reduce data security risk across email, cloud and endpoints

Deep visibility of user behavior

Proofpoint monitors how your workers interact with data across email, managed and unmanaged endpoints and cloud applications such as Microsoft 365, Google Workspace and Salesforce. We provide insights on user intent that help you appropriately respond to data risk. We also detect and prevent exfiltration of sensitive data. Examples are the copying of files to an unauthorized USB drive or attempted upload to a personal cloud folder.

Through integrations with LDAP and Active Directory, Proofpoint helps you define and dynamically apply granular email encryption policies. We also collect telemetry on the following behaviors:

- **File manipulation** — such as renaming files with sensitive data or changing their file extensions
- **Website and application usage** — such as downloading data backups or hacking tools from the web and installing them
- **Riskiest users' dangerous behaviors** — such as manipulating the Windows registry to disable security controls

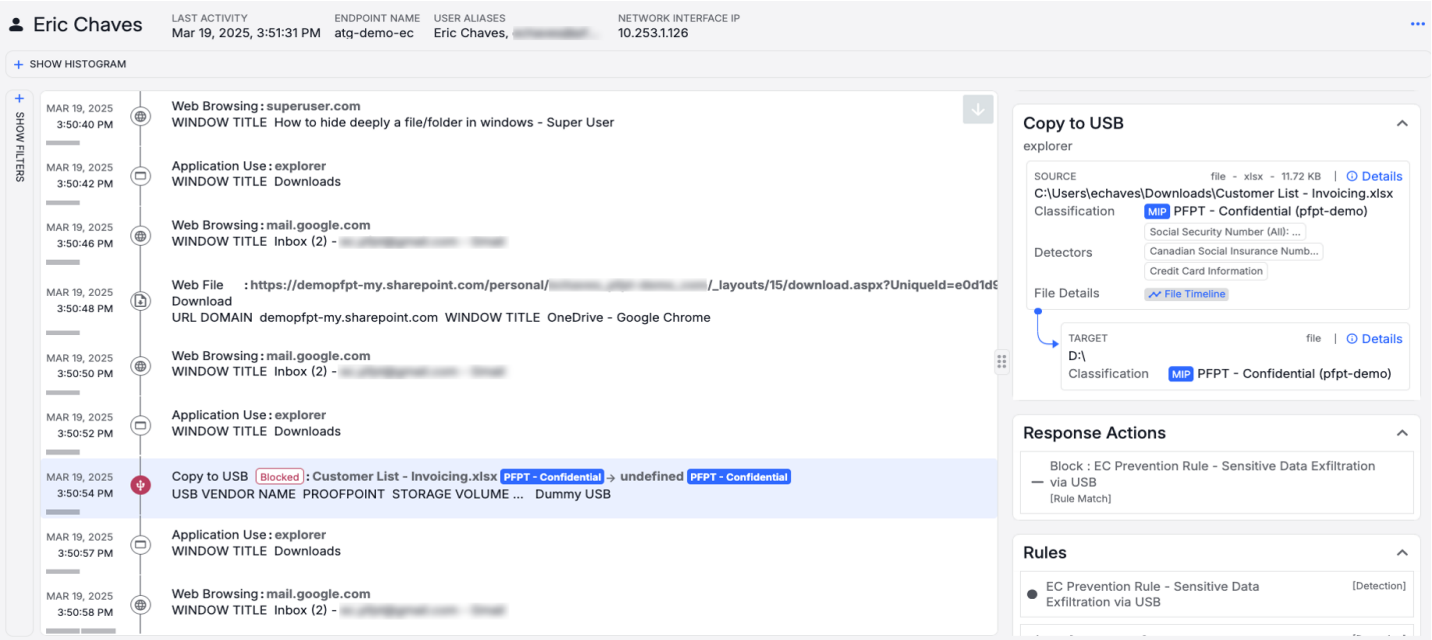

Figure 1: In this screenshot from the Data Security Workbench console, a user visits a website entitled "How to hide deeply a file/folder in Windows". The user then downloads a file from the company Sharepoint drive. Finally, the user copies a confidential file called "Customer List – invoicing.xlsx" to a USB drive. The timeline of user behavior and identification of sensitive content indicates to an analyst that the user is trying to circumvent company policy and that further investigation is required.

Accurate content identification

Proofpoint uses advanced content-identification methods to protect your data. For example, in the cloud, exact data matching and optical character recognition (OCR) can detect medical record numbers in images. This might help a healthcare provider, for instance, to reduce false positives and negatives.

You can create DLP policies that have large language model (LLM) classifiers. This protects newly developed, sensitive content without prior classification — and saves you time. By combining LLM classifiers with pattern matching, you can reduce false positives.

LLM-enriched alerts help to categorize documents. For example, if pattern matching for Social Security numbers triggers an alert, Proofpoint can identify whether the document is an income tax return, a patient form or a credit application. This accelerates your triage and investigations.

Adaptive policy enforcement

With insights into user behavior and the movement of sensitive data, you can respond to data risk with more accuracy. Proofpoint prevents the loss of sensitive data through GenAI prompts. Our solutions educate users about how to change their behaviors, enabling acceptable AI use. They automatically remediate the broad sharing of files in cloud applications. They also nudge a user to provide a justification for copying sensitive data to a cloud folder or to a network drive.

With adaptive policies, you can monitor high-risk users more closely. This gives you deeper context and better understanding of the intent of your users. Instead of manually adjusting policies, you can automate your responses to risky behaviors. With these dynamic policies, you can collect additional metadata and visual evidence of user activities when an alert is generated. With greater visibility and actionable insights, you save valuable investigation time and reduce your total cost of ownership.

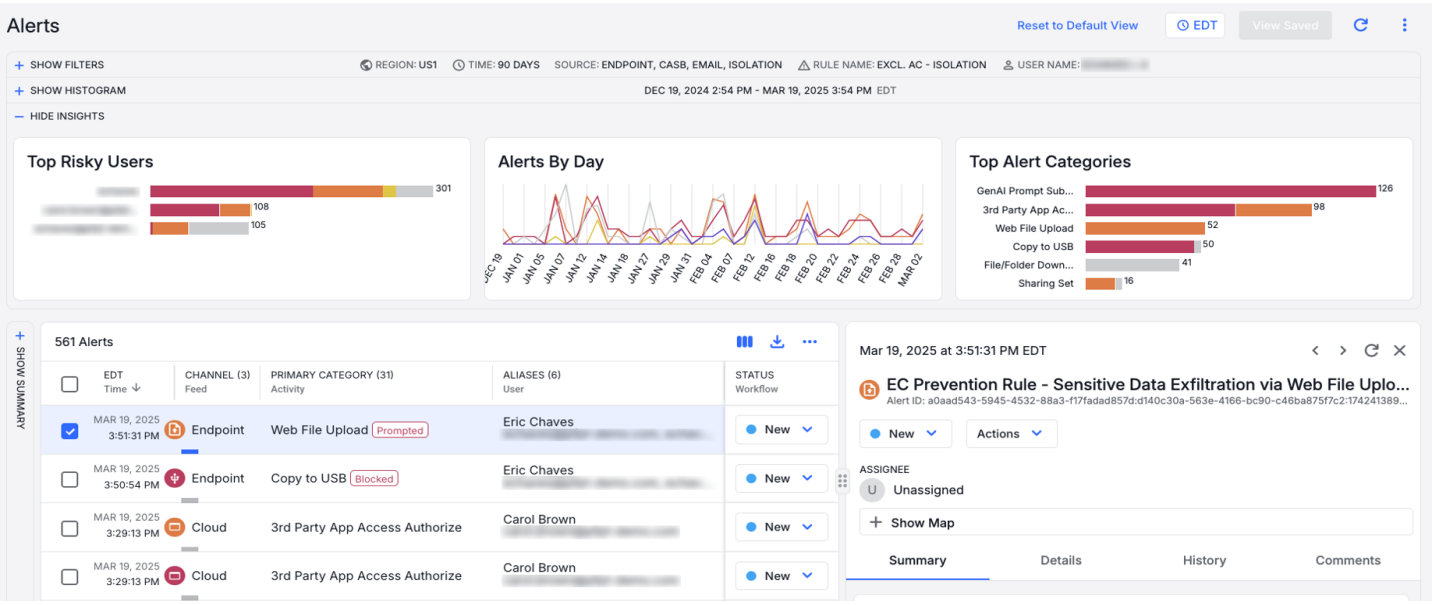

Figure 2: Data Security Workbench streamlines alert management across email, cloud and endpoints without making you switch between multiple consoles. In this example, an analyst has filtered alerts for a specific user. The workbench shows that the user uploaded sensitive data to their corporate email account and then tried to copy a file to a USB drive before being blocked.

Reduce operating costs and accelerate incident resolution

Efficient cross-channel DLP operations

Security teams that use legacy or siloed DLP tools can experience prolonged investigations and missed policy violations. To give you complete, cross-channel visibility of data risk in one place, Proofpoint gathers telemetry from cloud applications, endpoints and email. This streamlines the triaging of alerts across channels and accelerates investigation and response. The Data Security Workbench console provides powerful analytics, intuitive visualizations and efficient workflows that help you achieve the following:

- Investigate user interactions with data in a timeline view to determine intent and severity of risk (see figure 1)
- Triage and correlate alerts (see figure 2)
- Trace the lineage of a file as it is created, modified and shared
- Coordinate incident response
- Use out-of-the-box executive reports to demonstrate efficacy and coverage and generate custom reports for audit purposes
- Implement and manage consistent DLP policies and admin controls for data access and privacy across channels

Proactive data security

Data Security Workbench has a sophisticated search-and-filter feature. This helps you build custom explorations to proactively manage data risks. You can search for data exfiltration attempts and other risky activities, such as the use of unapproved GenAI apps. The timeline of user activities helps you understand the who, what, where, when and why behind each security incident.

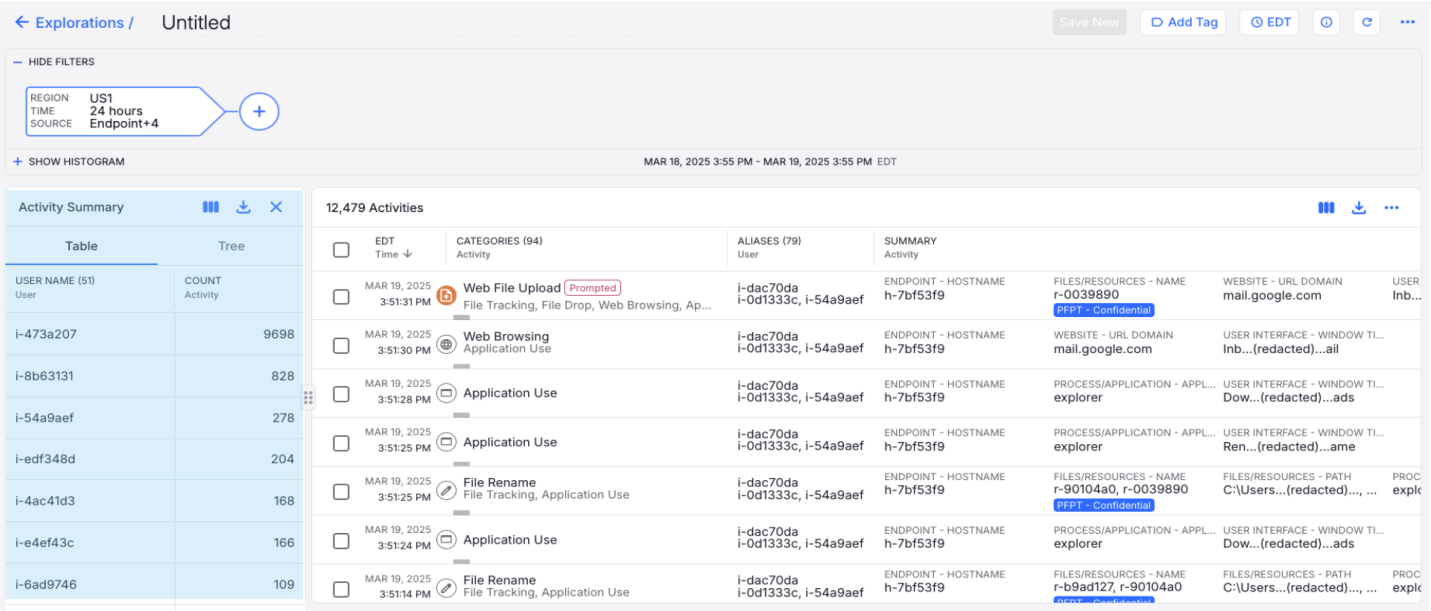

Figure 3: As highlighted, the console anonymizes user names. This ensures the privacy of users that are under investigation and removes analyst bias.

Enable business agility with a modern architecture

Available as services, our solutions save you valuable time. They deploy quickly, scale automatically and makes maintenance easy. They're modular, with shared services built in the cloud. Our multi-tenant cloud-native solutions are API-driven and highly scalable. They can support hundreds of thousands of users per tenant. The Proofpoint platform supports API integrations with ecosystem partners such as Microsoft, Okta, Splunk, ServiceNow and more.

Granular data privacy controls

While Proofpoint provides a global cloud-native console, it can store data in multiple regions. You can use attribute-based access controls to manage alerts and investigations across functions and regional roles. You can also mask sensitive data and anonymize user-identifying data (see figure 3). This helps you meet region-specific requirements for data privacy and residency.

Highly stable endpoint agent

Our lightweight user-mode agent is stable and quick to deploy. It's unique in its ability to detect data loss and improve your visibility of potential insider threats. By modifying the policies in the platform, you can change the behavior of the agent. Unlike kernel-mode agents, the Proofpoint agent provides a reliable user experience. This eliminates help desk tickets and saves your administrators time.

Shorten time to value with our expertise

Preventing data loss isn't easy. It requires technical and product knowledge and a deep understanding of data governance and stewardship. Proofpoint can be your trusted partner on the journey to a successful DLP program. Our applied services provide the expertise you need to optimize your technology investment, support your continuous operations and mature your data protection strategy.

Key features and capabilities of Proofpoint DLP solutions

Compare our solutions to find the right fit for your organization.

KEY FEATURES & CAPABILITIES	DLP TRANSFORM	DLP TRANSFORM ADVANCED	ADD-ONS
Deep user and file context	✓	✓	
Threat hunting for proactive detection/investigation	✓	✓	
Single user mode agent for insider threats and DLP	✓	✓	
Rich DLP detections (Regex, OCR, IDM, EDM) and MIP classification	✓	✓	
Monitor and detect file movements with data lineage	✓	✓	
Broad cloud application detectors	✓	✓	
Unified alert management and DLP configuration	✓	✓	
Granular data privacy and access controls	✓	✓	
Security ecosystem integration (SIEM/SOAR/Teams)	✓	✓	
Detect and analyze sensitive data in email messages and attachments		✓	
Dynamically encrypt external or internal-to-internal email		✓	
Fingerprinting of sensitive documents in email		✓	
AI-powered prevention of accidental and intentional data loss via email			✓
Discovery and classifying data stores			✓
Detect and remediate exposure risk in data stores			✓
Insider threat visual capture			✓

proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →

0201-034-01-02 3/25