

SOLUTION BRIEF

Proofpoint Data Security

Unified protection for data exfiltration,
data exposure and insider threats

Key benefits

- Comprehensive protection with the industry's first unified data security solution
- Reduced data security risk with omni-channel data loss prevention, insider threat management and data security posture management
- Streamlined security operations, faster time to security value, and lower cost of ownership
- Business agility through safe AI use and end-user productivity

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

Data doesn't lose itself

Data security risk today is based on human behavior. Modern workers put data at risk in many ways—whether through mistakes, malicious intent or account compromises. Proofpoint 2024 research showed that careless users caused 71% of data loss incidents. Departing employees accounted for 87% of cloud-based file exfiltration events.¹

Data sprawl is now a major challenge. Today's knowledge workers store data across public clouds, file-share services and on-premises databases. They also contribute data to large language models (LLMs). This fragmentation creates blind spots for IT and security teams. One in three breaches involves shadow data and results in a 16% higher average cost per breach.²

Many data security tools don't account for human behavior and intent. This means they can't distinguish safe activity from attempts at data theft. The result is false alerts, long investigations and inefficiency for security teams. According to Gartner, by 2027, 70% of Chief Information Security Officers (CISOs) in larger enterprises will adopt a consolidated approach to addressing both insider risk and data exfiltration.³

Reduce risk, lower costs and drive business agility

Proofpoint transforms data security with a human-centric and adaptive approach. It already helps 53 of the Fortune 100 reduce cybersecurity risk, lower operational costs and enable business agility.

Our unified solution protects against careless, malicious and compromised users with unmatched precision. It analyzes content and behavior across email, endpoints, software as a service (SaaS) applications and both cloud and on-premises data stores. Its adaptive and automated controls respond to emerging risks in real time. You get defense in depth against data exfiltration, exposure and insider threats.

70%

of CISOs will adopt a consolidated approach to addressing both insider risk and data exfiltration by 2027.

Source: Gartner

1. Proofpoint. *Data Loss Landscape Report*. 2024.
2. IBM and Ponemon Institute. *Cost of Data Breach Report*. 2025.
3. Gartner. *Market Guide for Data Loss Prevention*. 2025.

Products

- Proofpoint Enterprise DLP
- Proofpoint Data Security Posture Management
- Proofpoint Insider Threat Management
- Proofpoint Adaptive Email DLP

Reduced data security risk

Proofpoint's data security solution unifies data loss prevention (DLP), data security posture management (DSPM), and insider threat management (ITM). These unified components mean you can identify, monitor and mitigate data risks more effectively. With our solution, you can:

- **Transform your DLP program.**

The single-agent, unified console for Proofpoint DLP and Proofpoint ITM uses AI to accurately identify sensitive information. It spots risky behavior by understanding both content and context. It applies adaptive controls that address data exfiltration and insider risk across endpoints, email and the cloud.

- **Manage insider risk.** Proofpoint ITM adjusts monitoring and controls based on user risk. To speed up investigations, it captures clear evidence of user behavior.

- **Reduce data exposure.** Proofpoint DSPM uses in-place scanning to discover and classify sensitive data in cloud and hybrid environments. It helps you get visibility of data sprawl and reduce data exposure by removing excess privileges with a single click.

- **Defend against email data loss.** Proofpoint Adaptive Email DLP uses AI to detect and block misdirected emails, misattached files and emails to unauthorized accounts.

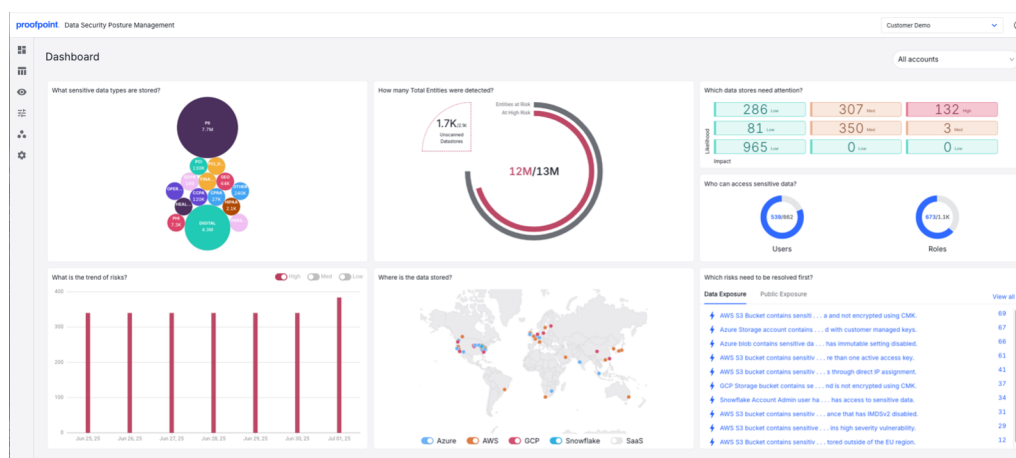


Figure 1: The DSPM dashboard shows types of valuable or sensitive data, its monetary value and risk, and who can access it.

AI-driven detection accuracy and faster time to value

- Using an **AI-powered, agentless scanner**, DSPM delivers the most accurate data classification in the market. By combining regular expression checking, natural language processing (NLP) and LLMs, it optimizes performance and minimizes resource use.
- Proofpoint Nexus AI classifiers** accurately identify document categories, such as source code, legal, accounting and HR. This keeps business-critical information protected.
- Anomaly detection** identifies unusual file changes and user activities across cloud and endpoints. This prevents data loss, insider threats and cloud account compromises.
- Adaptive Email DLP's **behavioral AI** stops data exfiltration to unauthorized accounts, misdirected emails and misattached files that rules-based email DLP can't catch.
- AI-assisted search** uses NLP to streamline explorations and speed up investigations.

Increased efficiency, reduced operational costs

With Proofpoint, you can improve the efficiency and agility of your data security and insider threat operations. This shortens time to security value and reduces total cost of ownership.

Efficient cross-channel operations

Powered by AI and intelligent automation, Proofpoint's adaptive and comprehensive solution boosts the efficiency of your data security program. Broad visibility, rich context and advanced analytics eliminate false positive alerts. Your security team gets more time to focus on strategic initiatives.

- Proofpoint human-centric security combines data telemetry with threat intelligence and insight into user behavior and intent. You can distinguish between safe and malicious data activity and respond to risks effectively.
- Proofpoint's unified policy engine enforces policies consistently across DLP, DSPM and ITM. Adaptive policies adjust as user risk changes.
- To help you prioritize risk mitigation, DSPM assesses the value of data, the likelihood and paths of potential attacks, and overprivileged access. One-click remediation of excess privileges prevents data exposure.
- Proofpoint Data Security Workbench helps you look for threats before they become breaches.

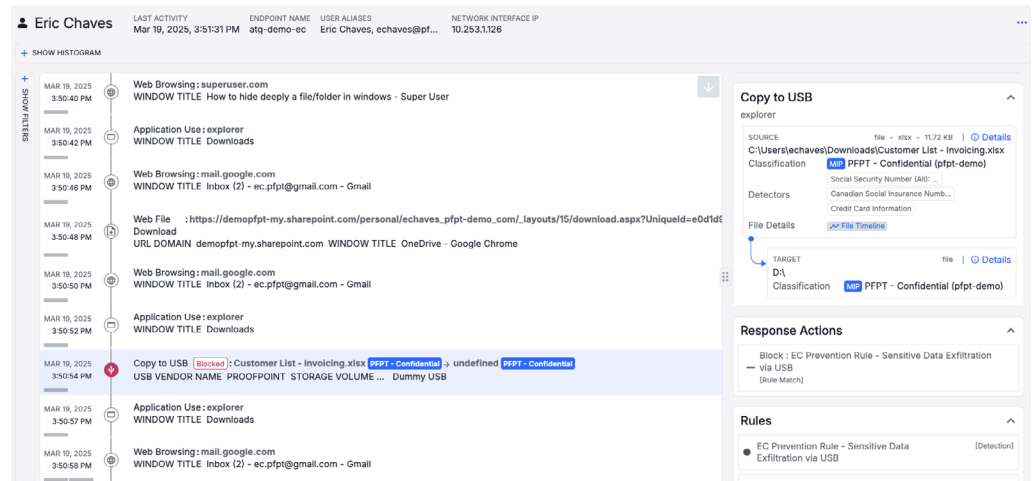


Figure 2: In this screenshot from the Data Security Workbench console, a user browses to a website titled “How to hide deeply a file/folder in Windows,” and then downloads a file from the company’s Sharepoint drive. Finally, they copy a confidential file “Customer List – invoicing.xlsx” to a USB drive. This timeline of user behavior and identification of sensitive content shows an analyst that this user is trying to circumvent company policy and that further investigation is required.

58%

Proofpoint reduces DLP administration costs by 58%.

Source: Enterprise Strategy Group

182%

Proofpoint Enterprise DLP gives a 182% return on investment over three years.

Source: Enterprise Strategy Group

Unmatched time to value and cost of ownership

The 2025 [Economic Validation of Proofpoint Enterprise DLP](#) by Enterprise Strategy Group found that Proofpoint reduces DLP administration costs by 58% and gives a 182% return on investment.⁴ The following capabilities enable these outcomes:

- Proofpoint's cloud-native service streamlines deployment, integration and administration.

- AI-driven data security with insights into user behavior shortens time to value from months to weeks compared to traditional solutions.
- Proofpoint's unified solution is more cost-effective and efficient than patchworks of standalone tools.
- DSPM identifies and removes redundant data and abandoned backups and snapshots. This reduces attack surfaces and lowers cloud storage costs.

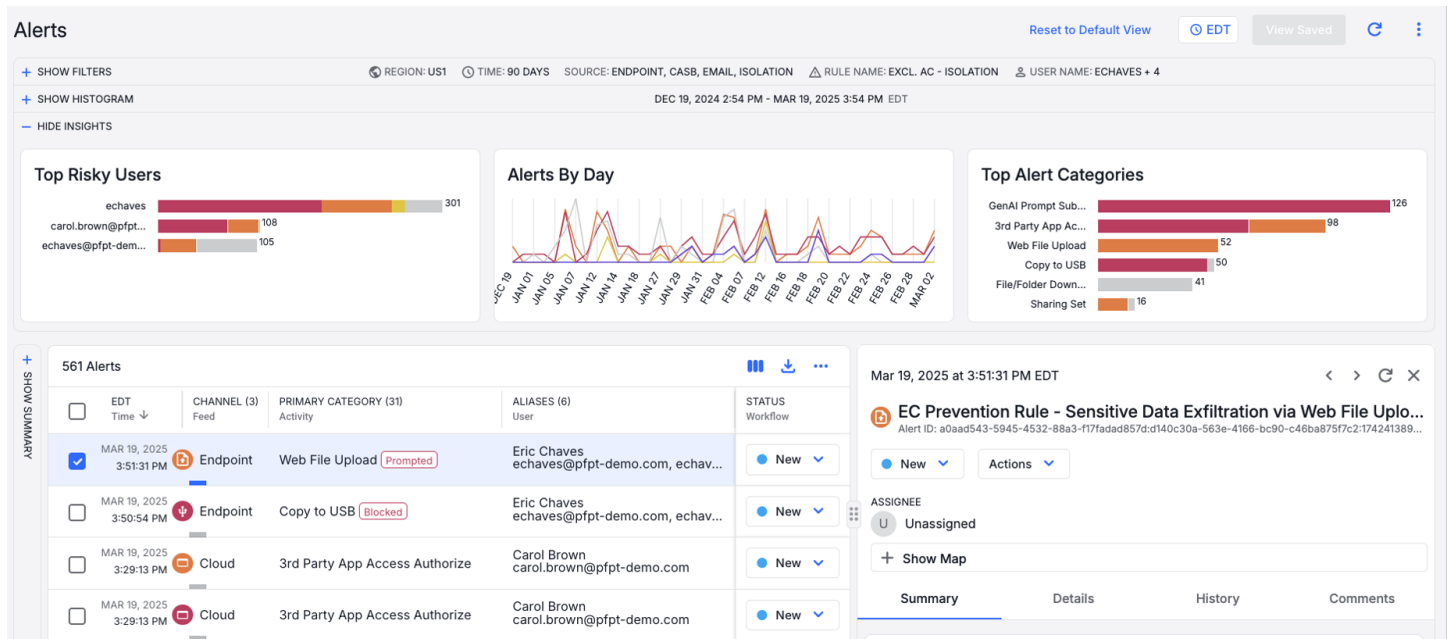


Figure 3: Data Security Workbench streamlines alert management across email, cloud and endpoints without the need for multiple consoles. In this example, an analyst filters alerts for a specific user. The dashboard shows that the user uploaded sensitive data to their corporate email account and tried to copy a file to a USB drive before being blocked.

4. Enterprise Strategy Group. *Analyzing the Economic Value of Proofpoint Enterprise DLP*. June 2025.

Agility in changing business environments

Whether your organization undergoes restructuring, expands geographically or adopts new technologies, Proofpoint Data Security keeps sensitive information protected. With Proofpoint, you can:

- **Support organizational change** by reducing risks to intellectual property, confidential information and other sensitive data. This includes information associated with mergers, acquisitions, or restructuring. With visibility of acquired organizations' environments, you can close inherited security gaps. Our automation helps apply and enforce security policies and standards. Adaptive policies adjust to fluctuating risk in real time.
- **Ensure safe and compliant AI use** by preventing sharing of sensitive data with public GenAI tools, custom large language models (LLMs) and AI agents. Restrict inclusion of protected information in GenAI prompts made through browsers or installed apps. Prevent the use of confidential data in custom LLM training.

- **Promote end-user productivity** by ensuring endpoint performance and application access. The single, lightweight user-mode agent for DLP and ITM avoids the software incompatibilities, system crashes and reduced endpoint performance associated with kernel-mode agents. Instead of broadly blocking applications, you can provide users with simple nudges. An example is a real-time reminder that sensitive information should not be included in a ChatGPT prompt. You can also prompt users to provide business justifications for copying sensitive data.

Maximize the impact of your data security and insider threat programs

As your strategic partner, Proofpoint is committed to helping make your program successful across people, processes and technology. Proofpoint Premium Services can help you optimize and mature your data security and insider threat programs. From consulting, technical advice and ongoing operational guidance to hands-on data security management, Proofpoint delivers the industry expertise you need, when you need it.



Figure 4: The Adaptive Email DLP insights dashboard shows statistics about email data loss detection and prevention. This includes metrics about email misdelivery, email exfiltration, custom policies applied, and users with the most anomalous behavior.

Proofpoint Data Security solution tiers

We offer the Proofpoint Data Security solution in three tiers: Data Security Core, Data Security Core Plus and Data Security Complete. Key features and capabilities of these solution tiers are shown in the table.

| KEY FEATURES & CAPABILITIES | DATA SECURITY CORE | DATA SECURITY CORE PLUS | DATA SECURITY COMPLETE |
|---|--------------------|-------------------------|------------------------|
| Deep user and file context | ✓ | ✓ | ✓ |
| Threat hunting for proactive detection and investigation | ✓ | ✓ | ✓ |
| Single user mode agent for insider threats and DLP | ✓ | ✓ | ✓ |
| Rich DLP detections (Regex, OCR, IDM, EDM) and MIP classification | ✓ | ✓ | ✓ |
| Monitoring and detection of 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) | ✓ | ✓ | ✓ |
| Detection and analysis of sensitive data in email messages and attachments | ✓ | ✓ | ✓ |
| Dynamic encryption of externally or internally-bound email | ✓ | ✓ | ✓ |
| Fingerprinting of sensitive documents in email | ✓ | ✓ | ✓ |
| Discovery and classification of data stores | | ✓ | ✓ |
| Detection and remediated risk exposure in data stores | | ✓ | ✓ |
| AI-powered prevention of accidental and intentional data loss through email | | | ✓ |



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: [X](#) | [LinkedIn](#) | [Facebook](#) | [YouTube](#)

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners. ©Proofpoint, Inc. 2025

DISCOVER THE PROOFPOINT PLATFORM →