Trellix

DATA SHEET

Trellix® Data Loss Prevention AI Data Risk Dashboard

Highlights

Track top AI tools: Understand the primary AI platforms where users share sensitive data from a catalog of 400+ predefined applications.

Identify exfiltration risks: Examine the top methods and vectors by which sensitive data is shared with AI platforms.

Track potential breaches: Quickly review incidents where data was allowed to leave the perimeter associated with AI platforms.

Detailed incident analysis: Use dynamic filtering to drill down into specific incidents to identify patterns and conduct in-depth analysis.

Instant remediation: Review and manage incident details, including evidence, directly from the dashboard with one click, creating a single workflow from detection to resolution.

Proactive AI data leak protection

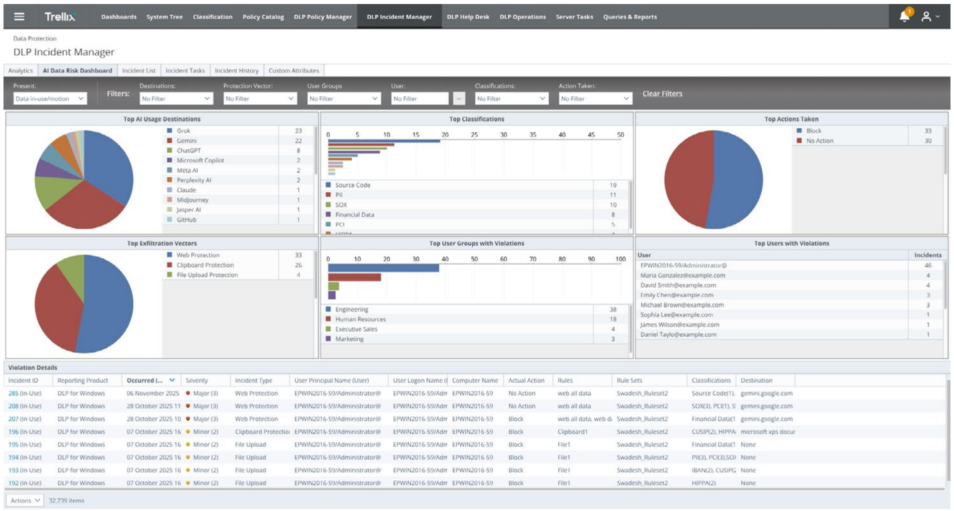
As AI adoption accelerates, organizations need insight into how and where users share sensitive information. The Trellix Data Loss Prevention (DLP) AI Data Risk Dashboard empowers organizations to securely adopt AI by identifying potential sensitive data leakage. Leveraging existing URL-based DLP policies, it provides the visibility needed to support compliance objectives and enforce AI usage policies across the enterprise.

- **Unified monitoring and deep visibility:** Identify high-risk data sharing activities, including copy/paste, clipboard sharing, and file uploads, using existing DLP policies to ensure sensitive data is not leaked into unauthorized LLMs or AI platforms. See Endpoint and Network events across Windows and macOS systems in a single view.
- **Proactive risk mitigation and control:** Address emerging challenges such as “Shadow AI” and rogue AI use by taking immediate action against unauthorized data sharing, enabling your team to block or monitor activity before it compromises corporate security, and manage potential incidents from within the dashboard.
- **Instant coaching for users:** Through DLP settings, provide immediate feedback to users who attempt to violate information-sharing policies. Use the dashboard to identify users and groups with the most violations to prioritize targeted outreach and retraining.
- **Dynamic compliance and regulatory support:** Use the dashboard’s granular data and reporting tools to achieve compliance with global AI regulations and your organization’s acceptable use polices. Dynamic filtering enables organizations to pinpoint critical data points where leaks may have occurred, investigate potential breaches, and track trends to fine-tune rule settings.

Growing AI data risks - know your numbers

- Security incidents involving “Shadow AI”—AI tools used without organizational approval or oversight—added an average of **$670,000** to the cost of a data breach.[1]
- **88%** of businesses report implementing AI officially in at least one business function[2]
- **80%** of organizations reported GenAI use in at least one business function[2]
- **Only 20%** of organizations feel confident in their ability to secure generative AI models[3]

- **Seamless integration and instant deployment:** Available as a free upgrade for existing Trellix DLP customers, the dashboard requires only a simple checkbox to enable, allowing you to activate advanced AI risk insights, based on your current DLP rules, without complex configurations or new agents**.**



Top AI Usage Destinations

■ Grok	23
■ Gemini	22
■ ChatGPT	8
■ Microsoft Copilot	2
■ Meta AI	2
■ Perplexity AI	2
■ Claude	1
■ Midjourney	1
■ Jasper AI	1
■ GitHub	1

Top Classifications

■ Source Code	19
■ PII	11
■ SOX	10
■ Financial Data	8
■ PCI	5

Top Actions Taken

■ Block	33
■ No Action	30

Top Exfiltration Vectors

■ Web Protection	33
■ Clipboard Protection	26
■ File Upload Protection	4

Top User Groups with Violations

■ Engineering	38
■ Human Resources	18
■ Executive Sales	4
■ Marketing	3

Top Users with Violations

User	Incidents
EPWIN2016-59/Administrator@	46
Maria Gonzalez@example.com	4
David Smith@example.com	4
Emily Chen@example.com	3
Michael Brown@example.com	3
Sophia Lee@example.com	1
James Wilson@example.com	1
Daniel Taylo@example.com	1

Violation Details

Incident ID	Reporting Product	Occurred (...	Severity	Incident Type	User Principal Name (User)	User Logon Name (I	Computer Name	Actual Action	Rules	Rule Sets	Classifications	Destination
285 (In-Use)	DLP for Windows	06 November 2025	● Major (3)	Web Protection	EPWIN2016-59/Administrator@	EPWIN2016-59/Adm	EPWIN2016-59	No Action	web all data	Swadesh_Ruleset2	Source Code(1),	gemini.google.com
208 (In-Use)	DLP for Windows	28 October 2025 11	● Major (3)	Web Protection	EPWIN2016-59/Administrator@	EPWIN2016-59/Adm	EPWIN2016-59	No Action	web all data	Swadesh_Ruleset2	SOX(3), PCI(1), S	gemini.google.com
207 (In-Use)	DLP for Windows	28 October 2025 10	● Major (3)	Web Protection	EPWIN2016-59/Administrator@	EPWIN2016-59/Adm	EPWIN2016-59	Block	web all data, web d	Swadesh_Ruleset2	Financial Data(1	gemini.google.com
196 (In-Use)	DLP for Windows	07 October 2025 16	● Minor (2)	Clipboard Protectio	EPWIN2016-59/Administrator@	EPWIN2016-59/Adm	EPWIN2016-59	Block	Clipboard1	Swadesh_Ruleset2	CUSIP(2), HIPPA	microsoft xps docur
195 (In-Use)	DLP for Windows	07 October 2025 16	● Minor (2)	File Upload	EPWIN2016-59/Administrator@	EPWIN2016-59/Adm	EPWIN2016-59	Block	File1	Swadesh_Ruleset2	Financial Data(1	None
194 (In-Use)	DLP for Windows	07 October 2025 16	● Minor (2)	File Upload	EPWIN2016-59/Administrator@	EPWIN2016-59/Adm	EPWIN2016-59	Block	File1	Swadesh_Ruleset2	PII(3), PCI(3),SO	None
193 (In-Use)	DLP for Windows	07 October 2025 16	● Minor (2)	File Upload	EPWIN2016-59/Administrator@	EPWIN2016-59/Adm	EPWIN2016-59	Block	File1	Swadesh_Ruleset2	IBAN(2), CUSIP(	None
192 (In-Use)	DLP for Windows	07 October 2025 16	● Minor (2)	File Upload	EPWIN2016-59/Administrator@	EPWIN2016-59/Adm	EPWIN2016-59	Block	File1	Swadesh_Ruleset2	HIPPA(2)	None

Figure 1. The AI Data Risk Dashboard enables organizations to identify potential sensitive data leakage.

The Trellix DLP AI Data Risk Dashboard is available with:

- Trellix DLP Endpoint Complete (on-premises, Windows version 11.14.0 or higher and macOS version 11.13.0 or higher)
- Trellix Network Prevent and Monitor (on-premises, versions 11.11.0 or higher)

To learn more about Trellix Data Loss Prevention, please visit http://trellix.com/dlp.

[1] IBM, Cost of a Data Breach Report 2025

[2] McKinsey, The state of AI in 2025: Agents, innovation, and transformation

[3] Accenture, State of Cybersecurity Resilience 2025