proofpoint.

SOLUTION BRIEF

Data Security for GenAI

Ensure safe generative AI use.

Key Benefits

- Gain visibility into unauthorised use of GenAI tools
- Prevent sensitive data exposure via enterprise GenAI tools and development using LLMs
- Enforce acceptable GenAI use policies in the cloud and on endpoints
- Monitor insider threats with dynamic policies for risky AI usage
- Train employees on acceptable use of GenAI tools

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

Generative AI (GenAI) offers immense potential, driving productivity, innovation and data insights. However, adoption also presents challenges, particularly in data security, privacy and compliance. Users risk exposing sensitive data and IP when using public GenAI tools, while weak governance can lead to unauthorised data access by enterprise tools, like Copilot for Microsoft 365, and misclassified sensitive outputs. Custom LLMs trained with customer data may disclose personally identifiable information (PII), raising compliance risks under regulations like GDPR, HIPAA and CCPA. Without strong governance, organisations face security breaches and fines due to regulatory non-compliance.

Proofpoint ensures acceptable use of GenAI tools and models through a comprehensive, human-centric approach that combines visibility, control and education. The Proofpoint Data Loss Prevention (DLP) solution monitors the use of GenAI on endpoints, providing insights into user interactions and identifying unauthorised tools. To prevent data loss, Proofpoint enforces policies that block or redact sensitive data inputs into GenAI prompts. Proofpoint Data Security Posture Management (DSPM) prevents data exposure via GenAI tools and LLMs by classifying and protecting sensitive data from unauthorised access. Additionally, ZenGuide offers tailored security awareness training to educate employees on safe GenAI practices, thereby fostering a culture of responsible usage. By integrating these strategies, Proofpoint safeguards organizations' sensitive data in the evolving GenAI landscape.

Gain visibility into the unauthorised use of GenAI tools

Proofpoint helps organisations understand who is using which GenAI tools and whether sensitive data is leaking into these tools or custom LLMs. Our data security report on AI usage highlights the sensitive data types submitted to public GenAI tools, most active users, top sites by activity and more (Figure 1).

Via Cloud APIs, you can identify and alert on third-party AI app authorisations such as OpenAI. You can also discover AI deployments in AWS Bedrock and Azure OpenAI that are using sensitive data.

Key Benefits

- Prevent sensitive data exposure via enterprise GenAI tools and development using LLMs

Prevent sensitive data exposure via GenAI tools and LLMs

Proofpoint DSPM discovers and classifies sensitive data in AI workflows, preventing exposure that could lead to breaches. It additionally protects data accessed by Microsoft Copilot by applying Microsoft Information Protection (MIP) labels, which are used to enforce protection policies, such as encryption and access controls.

It secures custom LLMs and AI applications on platforms like AWS Bedrock and Azure OpenAI by detecting sensitive data fed into foundational or custom models and Retrieval Augmented Generation (RAG) workflows.

Proofpoint provides specialised APIs for LLM security, enabling real-time sensitivity analysis of data flowing into and out of LLMs. These APIs offer full governance and visibility over data usage with seamless integration into customer workflows for effective deployment.

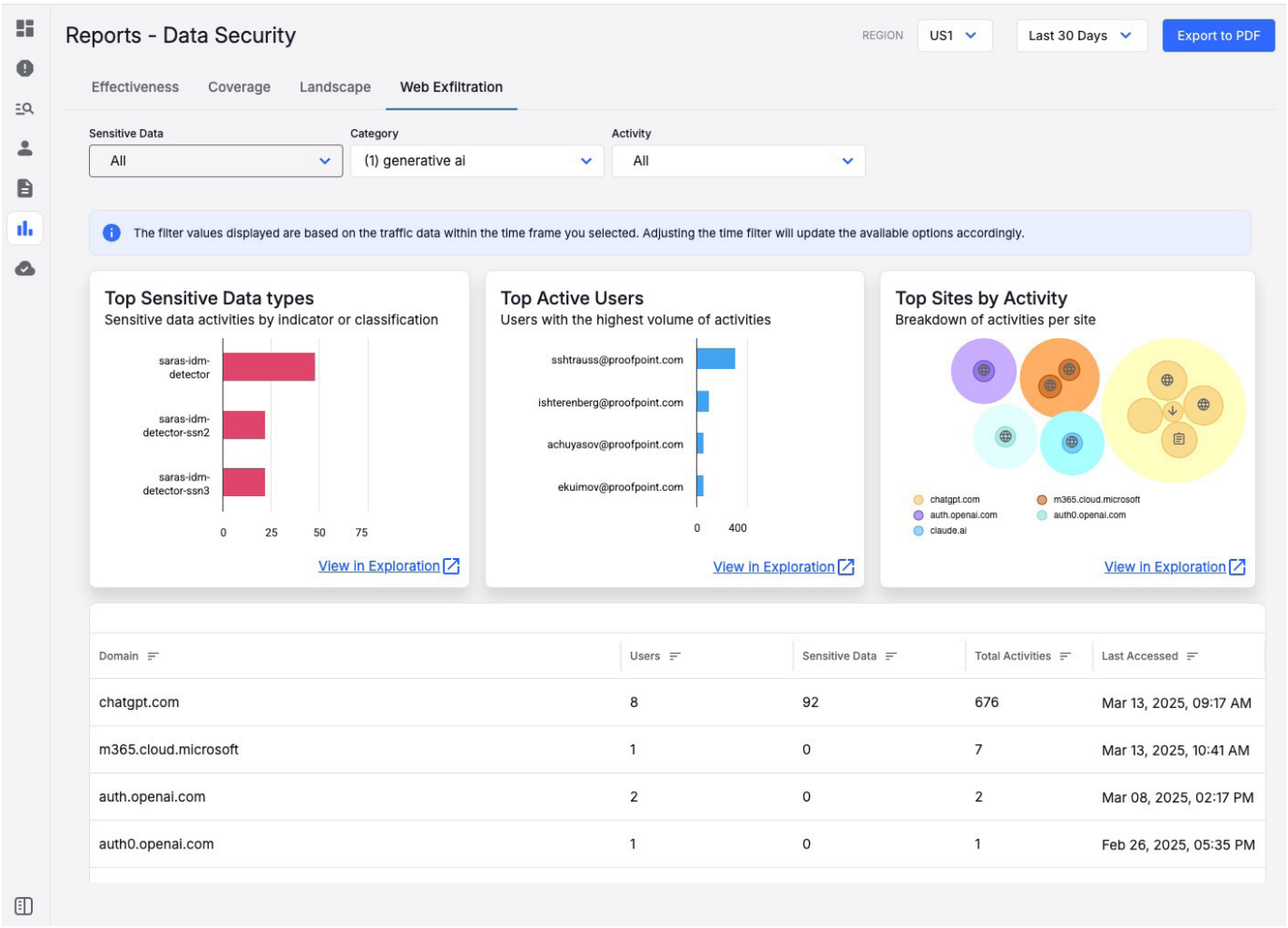

Figure 1: Report highlighting the top GenAI data exfiltration risks.

Key Benefits

- Enforce acceptable GenAI use policies in the cloud and on endpoints
- Monitor insider threats with dynamic policies for risky AI usage
- Train employees on acceptable use of GenAI tools

Defend against data loss and insider threats associated with GenAI use

On endpoints, you can monitor users browsing to GenAI sites using web categorisation or alert on unauthorised AI app installations. Our dynamic policies can elevate endpoint monitoring for users based on risky behaviors. For example, you can capture metadata and screenshots before and after users submit sensitive content to unauthorised GenAI sites. This helps you save time investigating user interactions with GenAI tools.

With Proofpoint DLP, you can enforce endpoint DLP policies for more than 600 GenAI tools by user, group or department and block web uploads to GenAI platforms or redact sensitive data input into prompts. To maintain user productivity, our solution can also nudge users to observe GenAI usage policies or ask them for a business justification instead of applying prevention policies.

Via Cloud APIs, we provide visibility into overshared files exposed to Microsoft 365 Copilot and alert your security team when users abuse Copilot to locate files containing sensitive information.

For example, Proofpoint detects when a risky insider uses Copilot to access many files containing sensitive data in a short time. Additionally, our solution classifies, labels and protects AI-generated content in cloud applications. It also revokes or blocks unapproved third-party AI app authorisations.

Educate employees on acceptable use of GenAI tools

Proofpoint educates users to safely use GenAI in your organisation. ZenGuide trains users with videos, posters, interactive modules and newsletters on safe data handling. ZenGuide enables you to leverage insights on your high-risk users and automate tailored, risk-based learning to targeted groups, such as developers, or to your riskiest users.

Training activities motivate safe behaviours through assessments, personalised nudges and coaching experiences. Activities include knowledge assessments, training assignments, notifications and policy acknowledgements, all designed to raise awareness and drive safe and acceptable use of GenAI tools.

Enabling the business with secure GenAI

Proofpoint delivers a human-centric solution to modern data security challenges. We provide insights into data exposure and loss risk from GenAI tools and LLM models.

With Proofpoint, you can easily balance user productivity with data security by adopting strategies that allow users access to GenAI tools and models with education, elevated monitoring and the right data controls.

proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' 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 cyberattacks. Leading organisations of all sizes, including 85 percent 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 →

0207-017-02-01 03/25