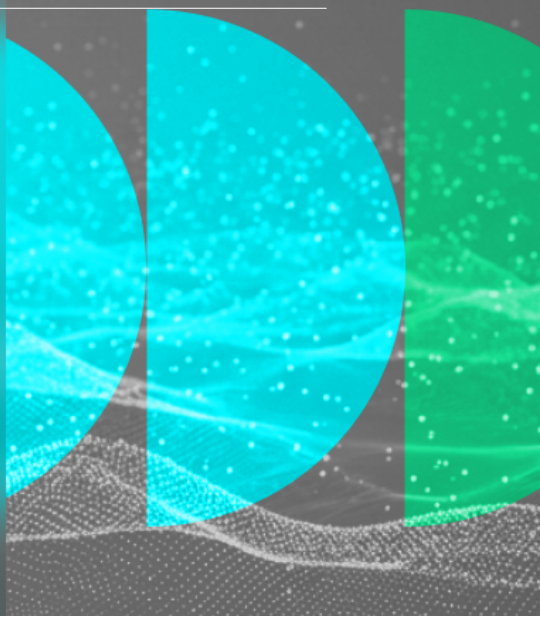
proofpoint.

SOLUTION BRIEF

Proofpoint Data Security for AI

Monitor and control sensitive data use across sanctioned and shadow AI applications



Key Benefits

- **Reduce AI-driven data risk**
- **Improve visibility into enterprise AI activity**
- **Monitor and govern shadow AI use**
- **Protect sensitive data in prompts and uploads**
- **Accelerate secure AI adoption**
- **Support compliance and audit readiness**

The Challenge: AI-Driven Data Exposure

Generative AI (GenAI) applications are transforming the enterprise, helping employees work faster and more efficiently. But organizations are also struggling to govern how sensitive data is shared with AI tools, copilots, and AI-powered applications.

Employees often upload files and submit prompts containing sensitive business information to sanctioned and shadow AI tools. Traditional data security technologies were not designed to monitor AI prompts, uploads, and responses in real time. This leaves organizations with limited visibility into how AI systems access and expose sensitive data.

Insiders can also misuse AI tools—intentionally or unintentionally—to find, summarize, rewrite, or exfiltrate sensitive information, including confidential documents, proprietary code, and intellectual property. Malicious insiders can use AI to accelerate data theft, evade traditional controls, or automate sensitive data extraction at scale.

Without the right controls, organizations risk data leakage, compliance violations, and unauthorized exposure of regulated or confidential information. Security teams need continuous visibility into AI data use and exposure, stronger policy enforcement, and comprehensive auditability to support safe AI adoption.

The Solution: Proofpoint Data Security for AI

Proofpoint helps organizations adopt AI securely with visibility into sanctioned and shadow AI data use. It unifies monitoring, AI-specific data controls, and activity insights to reduce risk and enable safe, scalable AI adoption.

Critical Capabilities

Visibility into AI data use and AI app posture

Proofpoint provides visibility into how employees and AI interact with enterprise data. Security teams can identify high-risk users, detect unsafe AI interactions, and understand what sensitive data and documents are exposed through sanctioned and shadow AI use.

The solution's autonomous custom classifiers identify organization-specific sensitive data shared through AI prompts, uploads, and generated responses, including intellectual property, source code, financial data, and strategic documents. This context enables more accurate detection, redaction, and protection across sanctioned and shadow AI applications.

Proofpoint continuously monitors AI and software as a service (SaaS) environments for misconfigurations, excessive site-level permissions, and insecure integrations. By uncovering excessive access rights and configuration weaknesses, organizations can remediate risks, reduce their attack surface, and prevent sensitive data from being exposed to users and AI apps.

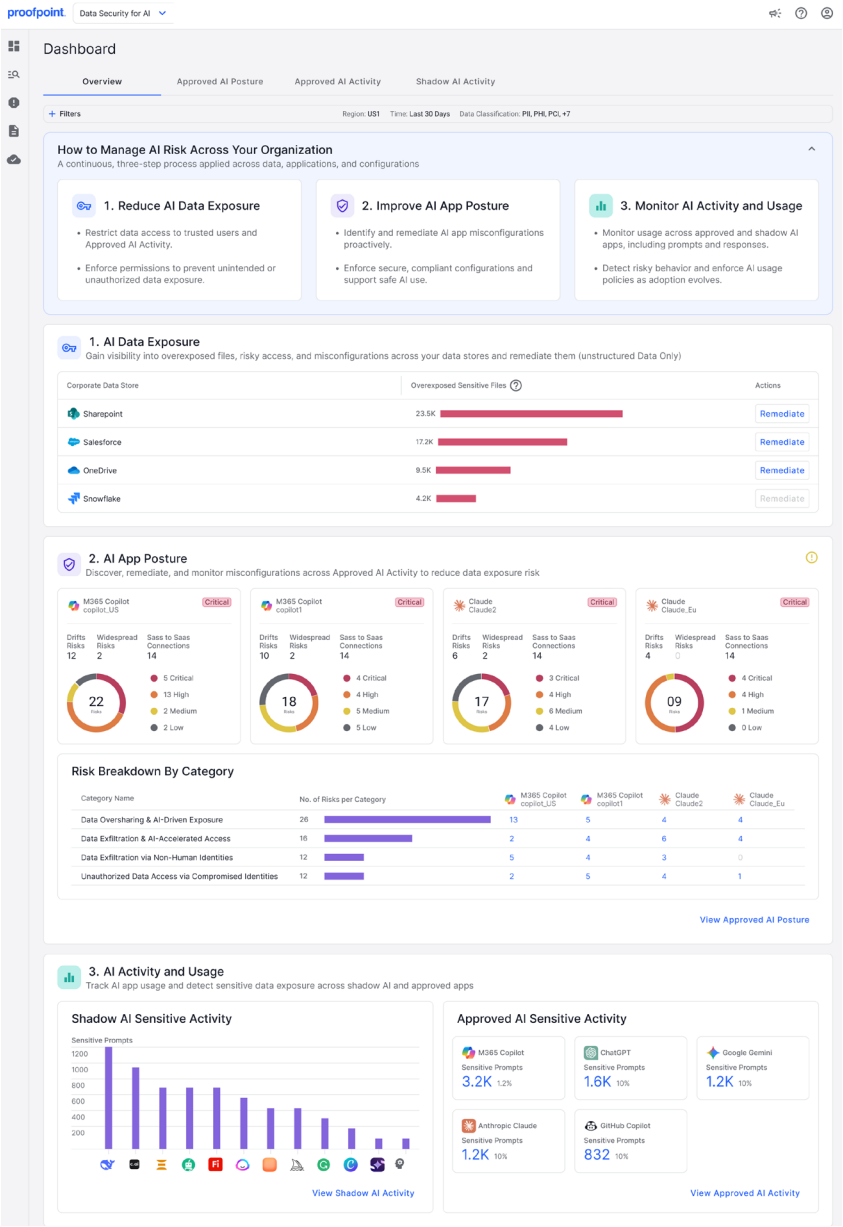


Figure 1: Proofpoint gives security teams deep visibility of how employees and AI tools interact with sensitive data.

Sanctioned AI monitoring and remediation

Proofpoint continuously monitors prompts, uploads, and AI-generated responses within sanctioned AI applications to identify sensitive data exposure and unusual insider activity. This includes excessive prompt activity or high-volume uploads. Full prompt and response capture supports investigations and audit readiness. Built-in remediation workflows help administrators and file owners quickly address overshared data.

Shadow AI data security

Organizations can reduce AI-driven data exposure by monitoring and controlling data use across shadow web and desktop AI applications. Proofpoint helps prevent data loss in prompts, uploads, and paste actions. It also redacts sensitive data in prompts before it is shared with AI tools. This helps organizations scale AI adoption securely without blocking AI applications entirely.

Operational Impact

Reduced AI-driven data loss

Help prevent sensitive data exposure across approved and shadow AI applications.

Improved AI visibility and governance

Gain centralized visibility into how employees and AI tools interact with enterprise data.

Safer enterprise AI adoption

Enable productive GenAI use while maintaining security, governance, and compliance controls.

Faster investigations and response

Capture AI activity, prompts, and responses to support investigations, remediation, and audit readiness.

Stronger compliance posture

Support evolving AI, privacy, and data protection requirements by enforcing policies for regulated, confidential, and proprietary information used with AI tools.

Reduced shadow AI risk

Discover and govern shadow AI use and risky user behavior while minimizing disruption to business productivity.

Learn More

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