

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. However, organisations 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 weren't designed to monitor AI prompts, uploads and responses in real time. This leaves organisations with limited visibility into how AI systems access and expose sensitive data.

Insiders can also misuse AI tools—intentionally or unintentionally—to find, summarise, 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, organisations risk data leakage, compliance violations and unauthorised 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 organisations 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 which sensitive data and documents are exposed through sanctioned and shadow AI use.

The solution's autonomous custom classifiers identify organisation-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, organisations can remediate risks, reduce their attack surface and prevent sensitive data from being exposed to users and AI apps.

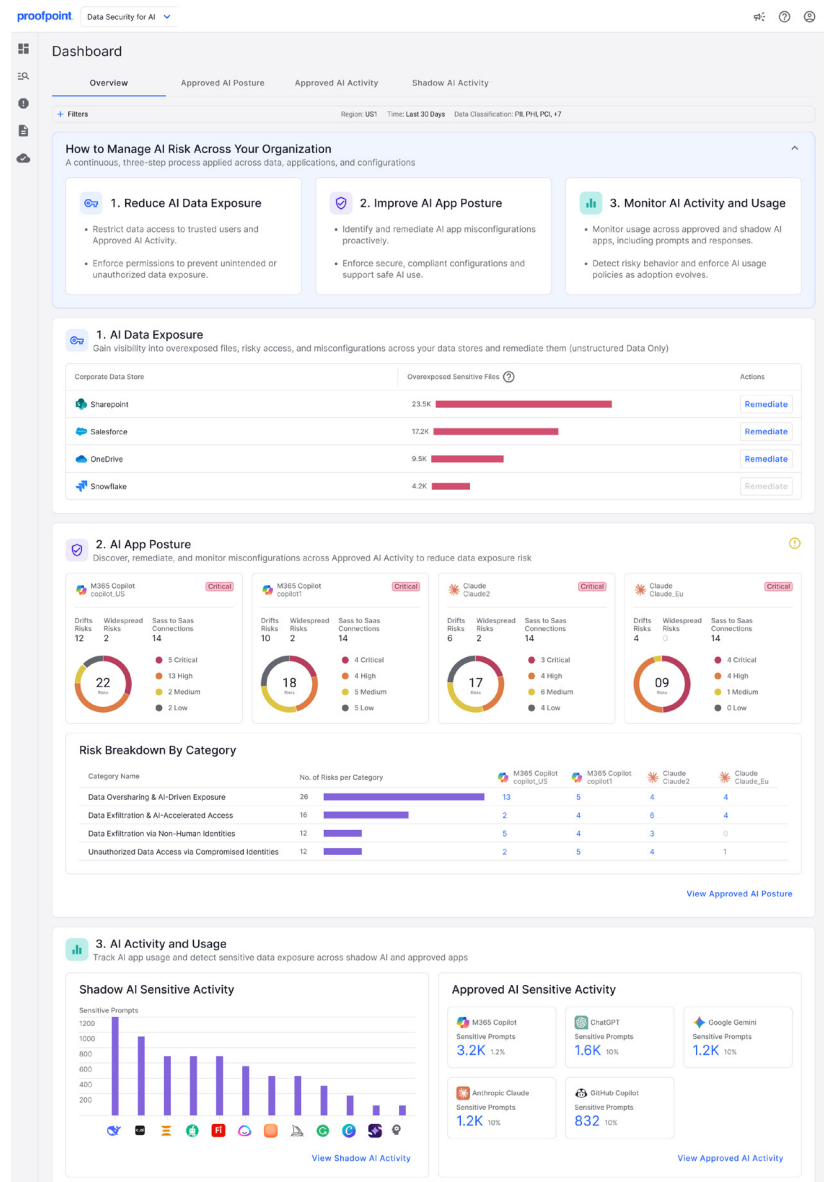


Figure 1: Proofpoint gives security teams comprehensive visibility into how employees and AI tools interact with sensitive data.

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

Organisations 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's shared with AI tools. This helps organisations 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 centralised 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 behaviour while minimising disruption to business productivity.

Learn More

For more information, visit proofpoint.com/uk

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises and millions of smaller organisations in stopping threats, preventing data loss and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organisations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com/uk

Connect with Proofpoint: [LinkedIn](#)

Proofpoint is a registered trademark or trade name of Proofpoint, Inc. in the United States and/or other countries. All other trademarks contained herein are the property of their respective owners.

LEARN MORE AT
PROOFPOINT.COM

Proofpoint Core Email Protection

Stop AI-scaled email threats with complete, continuous protection across the email lifecycle

Key Benefits

- Stop AI-scaled email threats before delivery
- 99.999% threat detection efficacy
- Deploy in 24 hours via API or secure email gateway (SEG)
- Complete pre-delivery, post-delivery, and click-time coverage
- Unified Threat Protection Workbench for faster investigations
- Best-of-breed ecosystem integrations

The Challenge: AI-Scaled Email Threats

Attackers iterate at machine speed. Frontier AI has removed the constraints that once limited how quickly threat actors could craft phishing lures, business email compromise (BEC) attacks, and social engineering campaigns. A single campaign now generates infinite, highly targeted variants that are personalized to each recipient.

These AI-generated threats arrive across email and collaboration channels with no typos, no reused templates, and no familiar fingerprints. Traditional defenses built on reputation lists and static signatures cannot keep pace. Meanwhile, 94% of human-targeted cyberattacks still begin with email.¹

These attacks exploit security gaps: missing pre-delivery protections, blind spots in supplier compromise detection, siloed cloud and collaboration environments, and a lack of account takeover controls.

AI is the Force Multiplier

What took an attacker 16 hours now takes 5 minutes. AI-generated phishing produces flawless, personalized lures with no telltale errors.



Infinite Variants
No two lures alike



Machine Speed
Campaigns in minutes



Multichannel
email, voice and video

¹ Source: Proofpoint threat research.

The Solution: Proofpoint Core Email Protection

Proofpoint Core Email Protection stops the broadest range of AI-scaled email threats with complete, continuous protection across the entire email lifecycle. Deploy via SEG or API for industry-leading 99.999% threat detection efficacy.

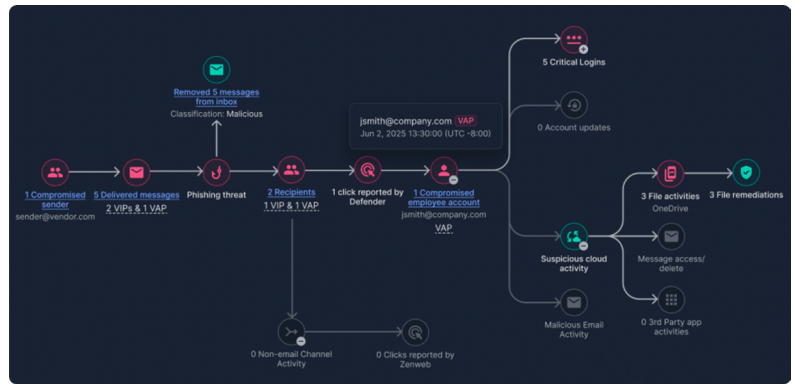


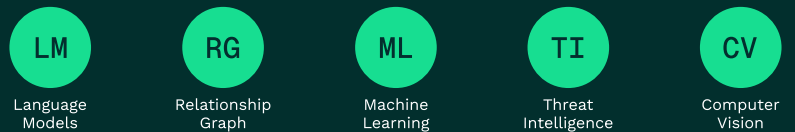
Figure 1. Threat Protection Workbench maps threats end-to-end.

Critical Capabilities

Nexus AI-powered detection

Proofpoint Nexus® uses language models, relationship graphs, machine learning, threat intelligence, and computer vision to detect the broadest range of advanced email threats with AI intent-based detections.

Proofpoint Nexus AI

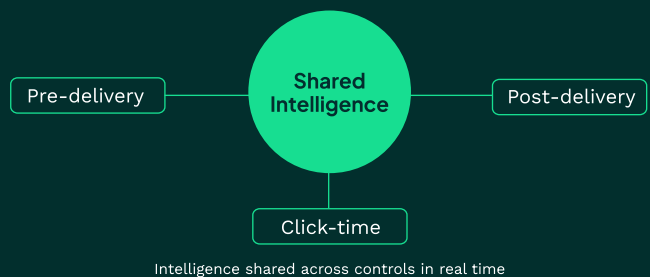


Unmatched Threat Data



Complete, continuous protection

Core Email Protection delivers coordinated defense across pre-delivery, post-delivery, and click time. Intelligence is shared across controls in real time, so a threat surfaced post-delivery sharpens the next pre-delivery decision.



Optional add-ons:



Unified SEG and API deployment

Proofpoint unifies market-leading SEG and API-based deployments into a single, integrated architecture. Our SEG helps stop inbound and outbound threats at the email gateway, while our API-based protection extends visibility and response to internal mail and post-delivery threats.

One console, one investigation workflow, and one set of policies replace the operational fragmentation of managing separate tools. Organizations deploy via API in as little as 24 hours, or combine SEG and API for maximum coverage.

Operational Impact

Here's what you can expect with Proofpoint.

Industry-leading detection efficacy

99.999% threat detection efficacy, with only 1 false positive per 19.7 million messages and 1 false negative per 5.3 million messages.

Faster time to value

API deployments complete in 24 hours. SEG and API together deliver defense-in-depth.

Reduced SOC burden

Automated workflows and visual attack chain investigation reduce analyst time on manual correlation.

Broader threat coverage

Get protection against external threats, post-delivery compromise, internal-to-internal phishing, and direct send.

Efficient security operations

With 99.999% of threats automatically stopped, security teams focus on the highest-priority investigations. The Threat Protection Workbench provides visual, end-to-end attack chain reconstruction, connecting messages, users, clicks, and remediation actions in a single view. Automated workflows, integrated search, and alert-based triage reduce mean time to remediation.

Future-proof architecture

Our integrated platform delivers automatic protection against newly discovered threats and emerging threat actors.

Best-of-breed integrations

Ecosystem integrations with CrowdStrike, Okta, Palo Alto Networks, Microsoft Defender, Splunk, and Sentinel.

Learn more at **proofpoint.com**

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com

Connect with Proofpoint: [LinkedIn](#)

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