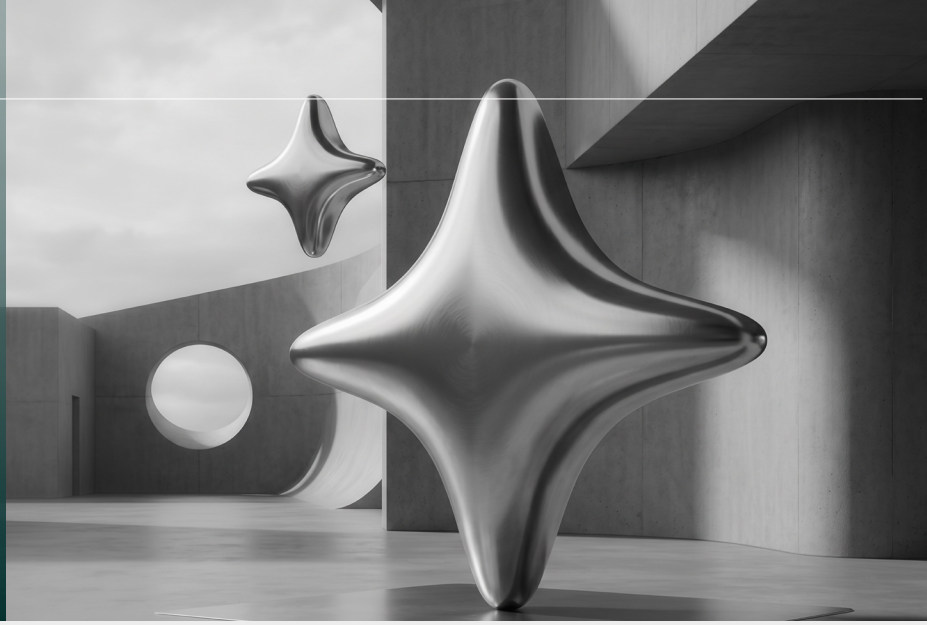
proofpoint.



SOLUTION BRIEF

AI at Proofpoint

AI is enabling new and innovative ways to help people get work done. Likewise, AI is helping threat actors boost their own productivity. Today, their tactics, techniques and procedures (TTPs) are amplified by AI, enabling them to deliver multistage, multichannel attacks on a global scale. These threats often bypass traditional security defences and are harder for users to identify on their own.

At the same time, risk doesn't only come from external attacks. Data exposure increasingly stems from everyday user behaviour inside the organisation. AI can help monitor the flow of data and identify risky behaviour in context. This can significantly reduce the burden on security operations centre (SOC) teams.

As the impact of AI on work evolves, Proofpoint is at the forefront of the industry when it comes to using AI to protect our customers. By combining continuous AI-driven innovation with unmatched threat intelligence, our solutions outpace threat actors, safeguard sensitive data and help organisations stay secure in an increasingly AI-powered world.

In 2025, Proofpoint saw a

94%

growth in the number of email threats targeting customers compared to the year before.

How threat actors are using AI to scale attacks

Proofpoint has witnessed first-hand the effects of AI when used by bad actors. In 2025, Proofpoint saw a 94% growth in the number of email threats targeting customers compared to the year before. This is leading to a more sophisticated threat landscape that includes AI prompt injection, email bombing and legitimate service abuse attacks.

Threat actors are using AI to gain traction in several ways:

- **Force multiplier.** AI enables threat actors to deliver more sophisticated attacks across a wider attack surface. This year, we've observed thousands of emails targeting AI agents to get them to act on behalf of the threat actor.
- **Reduced barrier to entry.** AI can automate 80–90% of the attack chain. This enables threat actors to spend time on more complex attacks. We've observed an increase in multistage, multichannel attacks that involve thousands of unwanted messages.
- **Advanced targeting.** Before AI, threat actors relied on predictable, generic templates for their attacks. With AI, they can create attacks that are personalised for each victim.

This year, we've seen an increase in personalised attacks abusing legitimate services.

All of these developments have made accurately identifying email threats more difficult.

Semantic analysis and other methods powered by large language models can help.

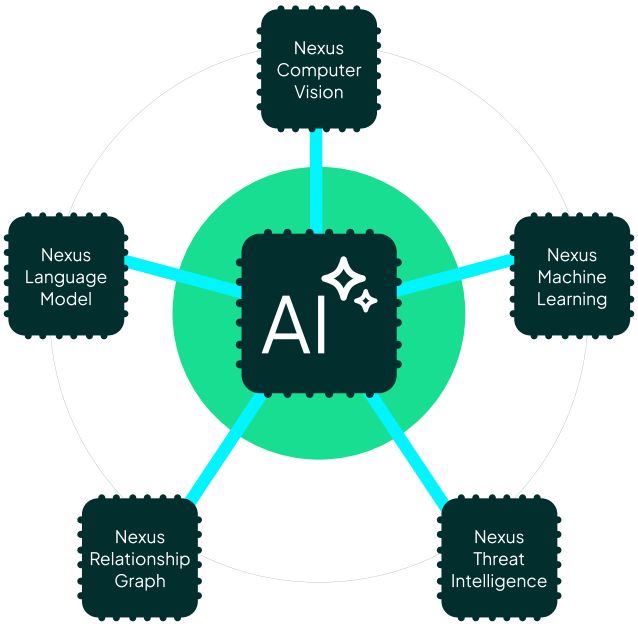
Proofpoint Nexus AI for Collaboration Security

Proofpoint's Collaboration Security Prime solutions leverage our Nexus™ AI platform, which uses a multilayered approach to threat detection.

How threat actors are using AI to scale attacks

Nexus is an ensemble of AI-powered engines working together to deliver 99.999% detection efficacy. It uses a combination of machine learning, computer vision, relationship graphs, threat intelligence and language models to accurately detect and block attacks.

Proofpoint Nexus's AI models process **2.1T emails** yearly, supported by a threat intelligence team that tracks **100+ unique threat actor groups** and more than **8,900 threat campaigns**.



Nexus LM™ (Language Model) detects BEC and sophisticated phishing threats, leveraging advanced language analysis (including transactional language, urgency, context and intent) to uncover hidden threats and unknown data risks.

Nexus RG™ (Relationship Graph) identifies subtle behavioural changes in your users' communications, detecting deviations in normal user behaviour, volumetric changes, sharing of sensitive company data to reduce risks of data leaks and protects against behaviour-driven cyber risks.

Nexus TI™ (Threat Intelligence) understands attackers' tactics and proactively protects against new cyberthreats by using real-time intelligence to identify emerging, attacker tactics and system vulnerabilities and trigger sandbox emulation for suspicious URLs and attachments.

Nexus CV™ (Computer Vision) identifies and neutralises vision-based threats. Through advanced computer vision technology, Nexus CV detects threats hidden in visual elements, such as phishing sites, QR codes, malicious attachments and spoofed emails.

Nexus ML™ (Machine Learning Model) uses dynamic and adaptive learning techniques, such as supervised learning, unsupervised learning and ensemble methods. It combines these techniques with predictive threat detection capabilities for mapping known attack behaviours and unsupervised techniques for detecting unknown abnormalities.

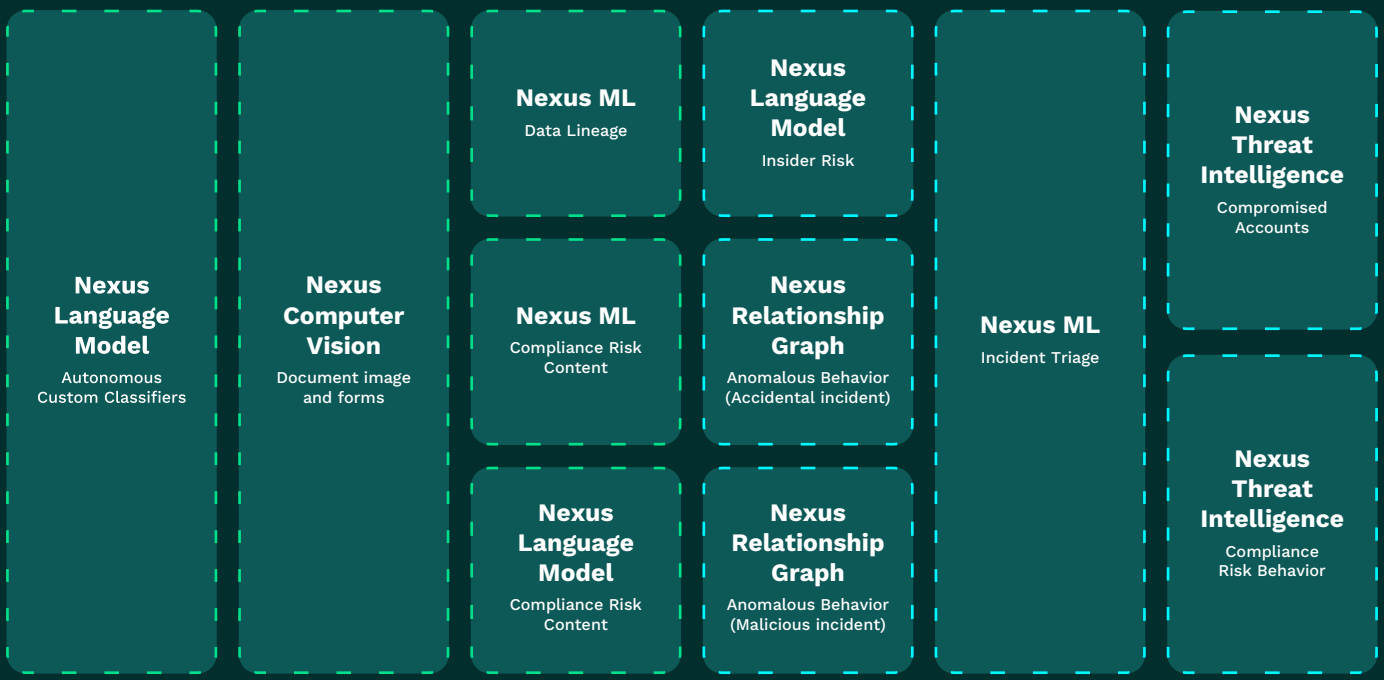
Proofpoint Nexus AI for Data Security and Governance

Proofpoint uses the same powerful market-leading Nexus engines to power our Data Security and Governance solutions.

AI to prevent data leaks

Nexus categorises and tracks the path of data and where it flows. It doesn't matter whether recipients are within an organisation or outside it.

- **Nexus LM™ (Language Model)** learns your organisation's real business document types, like deal materials, forecasts or product designs. It turns those learned classes into actionable policy context to quickly discover, prioritise and protect sensitive data without manual tuning.
- **Nexus RG™ (Relationship Graph)** understands relationships to prevent accidental and intentional data loss from misdirected emails and data exfiltration scenarios.
- **Nexus TI™ (Threat Intelligence)** protects against compromised accounts sending phishing emails both internally and externally.
- **Nexus CV™ (Computer Vision)** detects sensitive content in images within emails and documents.
- **Nexus ML™ (Machine Learning)** provides end-to-end visibility into how files are created, copied, renamed, shared and moved across repositories and destinations. It connects that activity into a traceable provenance timeline supporting faster investigations, origin-based controls and audit-ready evidence for data protection programmes.



Agentic AI at Proofpoint

When it comes to the agentic AI workspace, Proofpoint is investing in two key areas.

1: Proofpoint Satori™ agents

We're building AI agents to integrate with existing Proofpoint solutions. Satori agents will automate tasks and reduce the manual work of your SOC teams.

- **Abuse Mailbox Agent** automates manual review of reported messages. This reduces the burden on the SOC to distinguish between real threats and safe emails.
- **DLP Triage Agent** manages alerts and activity monitoring for your data loss prevention (DLP) solution.
- **Phishing Simulation Agent** uses AI automation to operationalise your security awareness programmes and boost human resiliency.

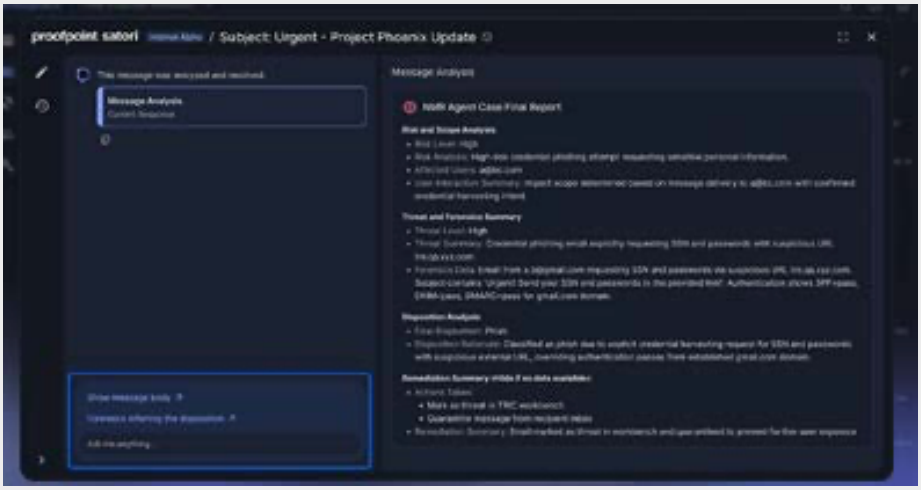


Figure 2: Proofpoint Satori Abuse Mailbox Agent in action.

2: Proofpoint AI Security

We understand the security risks introduced by rapid adoption of AI across users, agents and enterprise systems. That's why we've extended our human-centric security platform to govern and secure the entire agentic workspace.

Proofpoint AI Security provides unified visibility, control and protection across all AI interactions, ensuring safe and compliant use of AI technologies.

- **Secures how users, agents and systems interact with AI** across the enterprise
- **Provides end-to-end visibility and governance** across AI usage, agents and model interactions
- **Prevents data leakage, tool misuse and over-permissioned access** in AI workflows

proofpoint.