proofpoint.

AI at Proofpoint

AI is enabling new and innovative ways to help people get work done. At the same time, it's also 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.

But risk doesn't only come from external attacks. Data exposure increasingly stems from everyday user behaviour inside the organisation. That's where AI can help. It can monitor the flow of data and identify risky behaviour in context, which significantly reduces 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.

94%

Proofpoint saw email threats targeting customers rise by 94% in 2025.

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 the number of email threats targeting customers increase 94% 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 make them 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 involving 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 a rise in personalised attacks that abuse legitimate services.

All these developments have made it harder to accurately identify email threats. Semantic analysis and other methods powered by large language models can help.

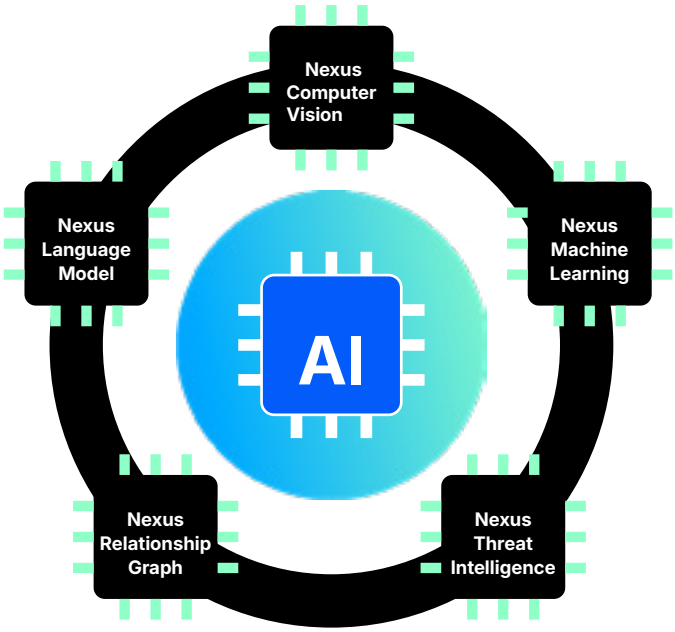
Proofpoint Nexus AI for Collaboration Security

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

AI to detect and block threats

Nexus is an ensemble of AI-powered engines that work 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's Nexus AI models process 2.3 trillion emails yearly, supported by a threat intelligence team that tracks 100+ unique threat actor groups and more than 8,400 active 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 and sharing of sensitive company data to reduce the risk of behaviour-driven attacks.

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 neutralisess 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 provide 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.

Nexus LM™ (Language Model) learns your organisation's real business document types, such as 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 to a traceable provenance timeline supporting faster investigations, origin-based controls and audit-ready evidence for data protection programmes.

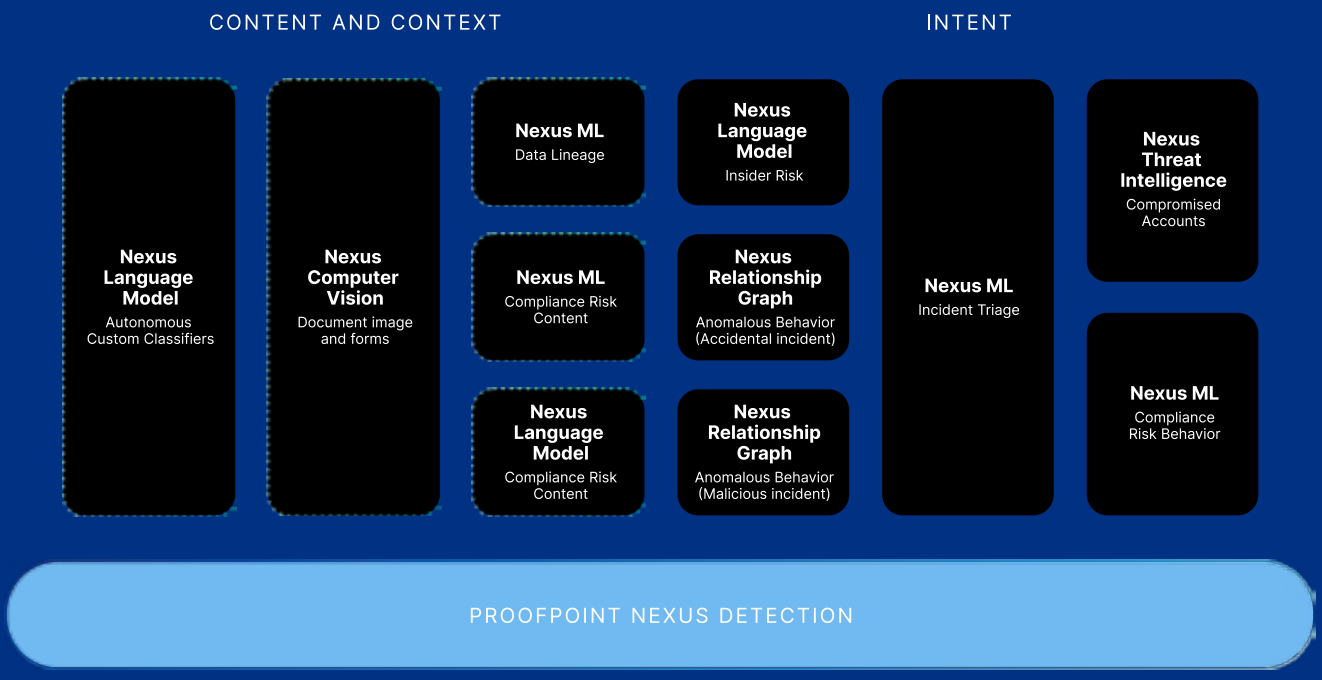


Figure 1. Nexus powers Data Security and Governance solutions.

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.

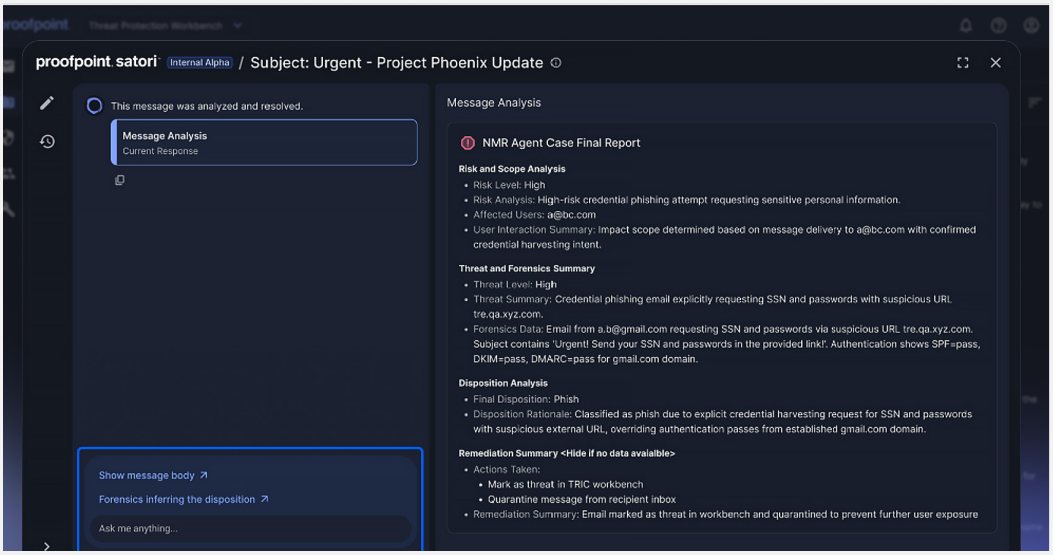


Figure 2. Proofpoint Satori Abuse Mailbox Agent in action.

2: Proofpoint Secure Agent Gateway

We understand the inherent security gaps that arise when implementing agentic AI workflows within your organisation. That's why we're extending our human-centric security platform to also secure all your agents.

Secure Agent Gateway secures existing agentic workflows and unifies agentic controls across all agents in your environment.

- **Secures sensitive information** flowing into and out of every agentic workflow
- **Is powered by our MCP** (Model Context Protocol) technology
- **Controls access to sensitive data** used by agents