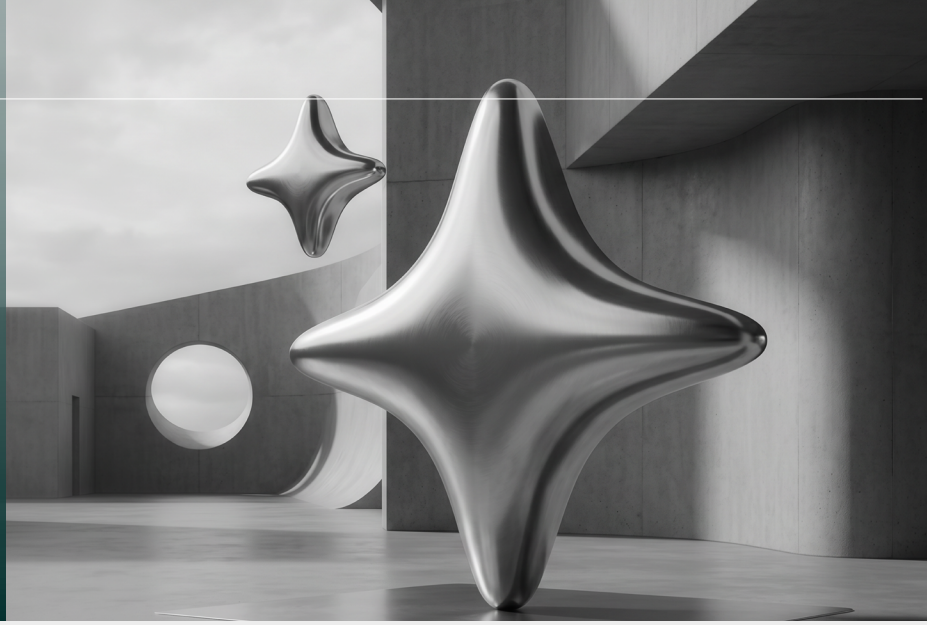
proofpoint.

RESUMO DA SOLUÇÃO

IA na Proofpoint



A IA está viabilizando maneiras novas e inovadoras de ajudar as pessoas a realizarem seu trabalho. Da mesma forma, a IA está ajudando os perpetradores de ameaças a aumentar sua própria produtividade. Hoje, suas táticas, técnicas e procedimentos (TTPs) são amplificados pela IA, permitindo-lhes realizar ataques de várias etapas e vários canais em escala global. Essas ameaças frequentemente contornam defesas de segurança tradicionais e são mais difíceis para os usuários identificarem por conta própria.

Ao mesmo tempo, o risco não vem apenas de ataques externos. A exposição de dados é, cada vez mais, resultado do comportamento diário dos usuários dentro da organização. A IA pode ajudar a monitorar o fluxo de dados e a identificar comportamentos arriscados no contexto. Isso pode reduzir significativamente a carga sobre as equipes do centro de operações de segurança (SOC).

Enquanto o impacto da IA no trabalho evolui, a Proofpoint está na vanguarda do setor no que se refere ao uso de IA para proteger nossos clientes. Ao combinar inovação contínua impulsionada por IA com inteligência sobre ameaças inigualável, nossas soluções superam os perpetradores de ameaças, protegem dados confidenciais e ajudam as organizações a permanecerem seguras em um mundo cada vez mais impulsionado por IA.

Em 2025, a Proofpoint observou um crescimento de

94%

no número de ameaças por e-mail direcionadas a clientes em comparação ao ano anterior.

Como os perpetradores de ameaças estão usando IA para ampliar ataques

A Proofpoint testemunhou em primeira mão os efeitos da IA quando utilizada por elementos maliciosos. Em 2025, a Proofpoint registrou um crescimento de 94% no número de ameaças por e-mail direcionadas a clientes em comparação com o ano anterior. Isso está levando a um cenário de ameaças mais sofisticado que inclui ataques de injeção de prompts de IA, bombardeio de e-mails e abuso de serviços legítimos.

Os perpetradores de ameaças estão usando IA para ganhar terreno de várias maneiras:

- **Multiplicadora de força.** A IA permite que os perpetradores de ameaças realizem ataques mais sofisticados em uma superfície de ataque maior. Este ano, observamos milhares de e-mails direcionados a agentes de IA para fazê-los agir em nome do perpetrador da ameaça.
- **Barreira de entrada reduzida.** A IA pode automatizar de 80 a 90% da cadeia de ataque. Isso permite aos perpetradores de ameaças investir seu tempo em ataques mais complexos. Observamos um aumento em ataques de várias etapas e vários canais que envolvem milhares de mensagens indesejadas.
- **Direcionamento avançado.** Antes da IA, os perpetradores de ameaças dependiam de modelos previsíveis e genéricos para seus ataques. Com a IA, eles podem criar ataques personalizados para cada vítima.

Este ano, vimos um aumento em ataques personalizados que abusam de serviços legítimos.

Todos esses desdobramentos tornaram mais difícil a identificação precisa de ameaças por e-mail.

A análise semântica e outros métodos impulsionados por grandes modelos de linguagem podem ajudar.

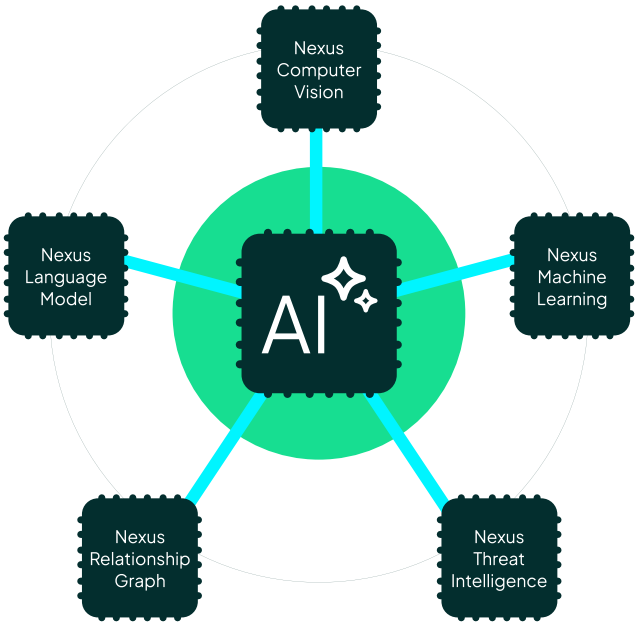
Proofpoint Nexus AI para segurança de colaboração

As soluções Proofpoint Collaboration Security Prime utilizam nossa plataforma Proofpoint Nexus™ AI, que emprega uma abordagem em várias camadas para detecção de ameaças.

Como os perpetradores de ameaças estão usando IA para ampliar ataques

O Proofpoint Nexus é um conjunto de mecanismos alimentados por IA que trabalham em conjunto para oferecer uma eficácia de detecção de 99,999%. Ele utiliza uma combinação de autoaprendizagem, visão computacional, gráficos de relacionamento, inteligência sobre ameaças e modelos de linguagem para detectar e bloquear ataques com precisão.

Os modelos do Proofpoint Nexus AI processam **2,1 trilhões de e-mails** por ano, com o suporte de uma equipe de inteligência sobre ameaças que monitora **mais de 100 grupos de perpetradores de ameaças distintos** e mais de **8.900 campanhas de ameaças.**



O Nexus LM™ (Language Model) detecta BEC e ameaças sofisticadas de phishing, aproveitando uma análise avançada de linguagem (incluindo linguagem transacional, senso de urgência, contexto e intenção) para descobrir ameaças ocultas e riscos desconhecidos para os dados.

O Nexus RG™ (Relationship Graph) identifica mudanças comportamentais sutis nas comunicações dos usuários, detectando desvios em relação ao comportamento normal, alterações de volume e compartilhamento de dados confidenciais da empresa para reduzir os riscos de vazamento de dados e proteger contra riscos cibernéticos baseados em comportamento.

O Nexus TI™ (Threat Intelligence) entende as táticas dos atacantes e protege proativamente contra novas ameaças cibernéticas utilizando inteligência em tempo real para identificar táticas emergentes de atacantes e vulnerabilidades de sistema e acionar emulação em área restrita (sandbox) para URLs e anexos suspeitos.

O Nexus CV™ (Computer Vision) identifica e neutraliza ameaças baseadas em visão. Por meio de tecnologia avançada de visão computacional, o Nexus CV detecta ameaças ocultas em elementos visuais, como sites de phishing, códigos QR, anexos maliciosos e e-mails falsificados.

O Nexus ML™ (Machine Learning) utiliza técnicas de autoaprendizagem dinâmicas e adaptáveis, como aprendizagem supervisionada, aprendizagem não supervisionada e métodos de conjunto. Ele combina essas técnicas com capacidades preditivas de detecção de ameaças para mapear comportamentos de ataque conhecidos e técnicas de aprendizagem não supervisionada para detectar anormalidades desconhecidas.

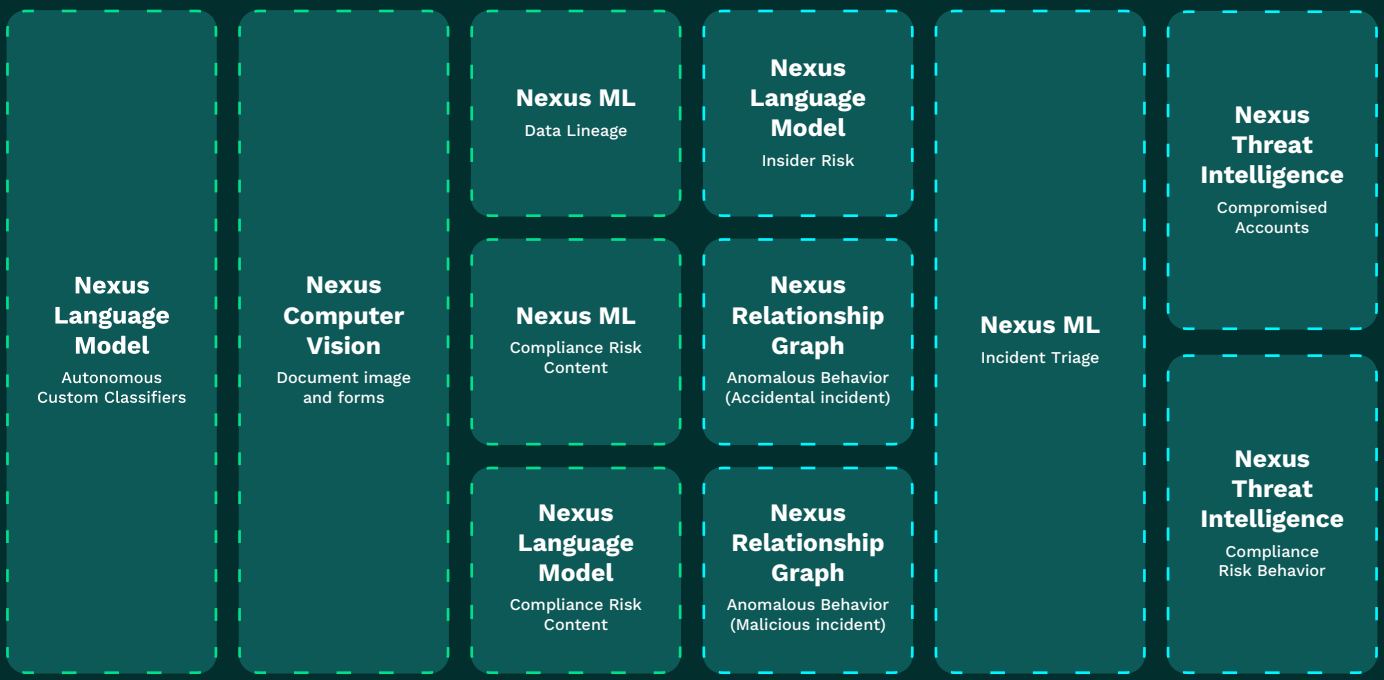
Proofpoint Nexus AI para segurança e governança de dados

A Proofpoint utiliza os mesmos poderosos mecanismos Nexus líderes de mercado para impulsionar nossas soluç ões de segurança e governança de dados.

IA para evitar vazamentos de dados

O Proofpoint Nexus categoriza e rastreia o caminho dos dados e para onde eles fluem. Não importa se os destinatários estão dentro ou fora da organização.

- **O Nexus LM™ (Language Model)** aprende os tipos de documentos empresariais específicos da sua organização, como materiais de negociação, previsões ou projetos de produtos. Ele transforma essas classes aprendidas em um contexto de política decisiva para descobrir, priorizar e proteger rapidamente dados confidenciais, sem ajustes manuais.
- **O Nexus RG™ (Relationship Graph)** compreende os relacionamentos para evitar perda acidental ou intencional de dados por e-mails endereçados incorretamente e cenários de vazamento de dados.
- **O Nexus TI™ (Threat Intelligence)** protege contra contas comprometidas que enviam e-mails de phishing, tanto internamente quanto externamente.
- **O Nexus CV™ (Computer Vision)** detecta conteúdo confidencial em imagens dentro de e-mails e documentos.
- **O Nexus ML™ (Machine Learning)** oferece visibilidade completa sobre como os arquivos são criados, copiados, renomeados, compartilhados e movidos entre repositórios e destinos. Ele conecta essa atividade a uma cronologia de proveniência rastreável que viabiliza investigações mais rápidas, controles baseados na origem e evidências prontas para auditoria em programas de proteção de dados.



IA agêntica na Proofpoint

Em se tratando de espaço de trabalho de IA agêntica, a Proofpoint está investindo em duas áreas-chave.

1. Proofpoint Satori™ Agents

Estamos desenvolvendo agentes de IA para integrar com as soluções existentes da Proofpoint. Os agentes Proofpoint Satori Agents automatizam tarefas e reduzem o trabalho manual das equipes do SOC.

- **O Abuse Mailbox Agent** automatiza a revisão manual das mensagens denunciadas. Isso reduz o trabalho do SOC de distinguir entre ameaças reais e e-mails seguros.
- **O DLP Triage Agent** gerencia alertas e o monitoramento de atividades para a sua solução de prevenção de perda de dados (DLP).
- **O Phishing Simulation Agent** utiliza automação com IA para operacionalizar seus programas de conscientização de segurança e aumentar a resiliência humana.

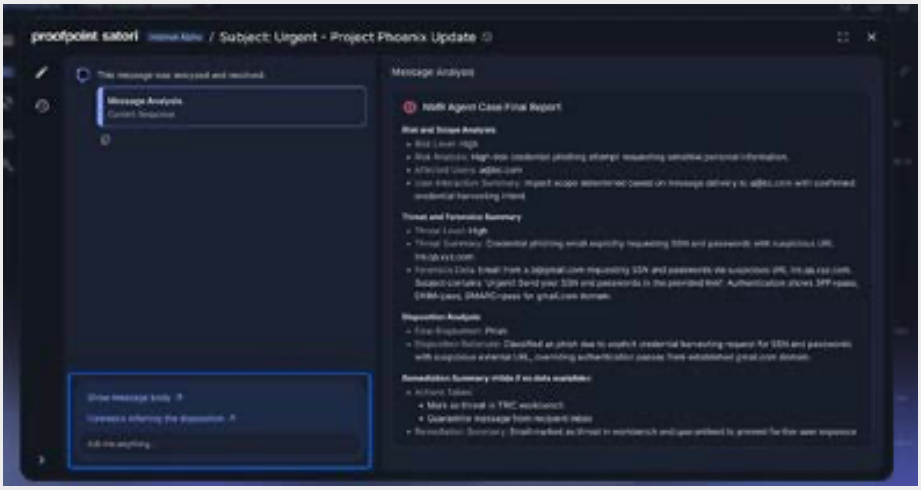


Figura 2. O Proofpoint Satori Abuse Mailbox Agent em ação.

2. Proofpoint AI Security

Entendemos os riscos de segurança introduzidos pela adoção rápida de IA entre usuários, agentes e sistemas empresariais. Por isso ampliamos nossa plataforma Human-Centric Security para governar e proteger todo o espaço de trabalho agêntico.

O **Proofpoint AI Security** oferece visibilidade, controle e proteção unificados em todas as interações com IA — garantindo que o uso de tecnologias de IA seja seguro e em conformidade.

- **Protege a forma como usuários, agentes e sistemas interagem com IA** em toda a empresa
- **Oferece visibilidade e governança completas** sobre o uso de IA, agentes e interações com modelos
- **Evita vazamento de dados, uso indevido de ferramentas e acesso excessivamente permissivo** em fluxos de trabalho de IA