proofpoint.

# IA na Proofpoint

A IA está viabilizando maneiras novas e inovadoras de ajudar as pessoas a realizarem seu trabalho. Ao mesmo tempo, também está ajudando perpetradores de ameaças a aumentar sua própria produtividade. Hoje, suas táticas, técnicas e procedimentos (TTPs) são amplificados pela IA, permitindo que eles realizem 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.

Porém, o risco não é consequência apenas de ataques externos. A exposição de dados é, cada vez mais, resultado do comportamento diário dos usuários dentro da organização. É aí que a IA pode ajudar. Ela pode monitorar o fluxo de dados e identificar comportamentos de risco no contexto, o que reduz 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 da indústria quando se trata de usar a IA para proteger nossos clientes. Ao combinar inovação contínua impulsionada por IA com inteligência sobre ameaças inigualável, nossas soluções superam perpetradores de ameaças, protegem dados confidenciais e ajudam as organizações a permanecer seguras em um mundo cada vez mais impulsionado por IA.

**94%**

**A Proofpoint observou que as ameaças por e-mail direcionadas a clientes aumentaram 94% em 2025.**

## Como os perpetradores de ameaças estão usando a IA para ampliar ataques

A Proofpoint testemunhou em primeira mão os efeitos da IA quando usada por elementos maliciosos. Em 2025, a Proofpoint observou um aumento de 94% na quantidade de ameaças por e-mail direcionadas a clientes em comparação com o ano anterior. Isso está resultando em um cenário de ameaças mais sofisticado que inclui injeção de prompts de IA, bombardeio de e-mail e ataques de abuso de serviços legítimos.

Perpetradores de ameaças estão usando a 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 se aproveitam 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.

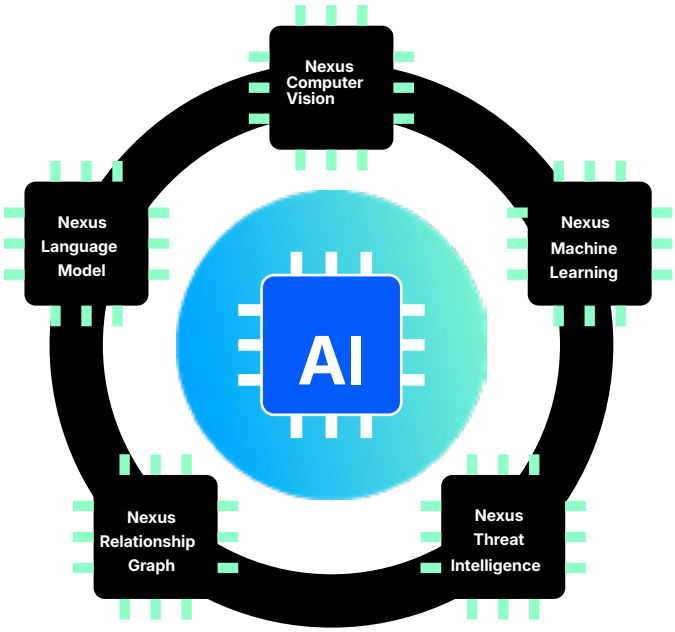
# Proofpoint Nexus AI para segurança de colaboração

As soluções **Proofpoint Collaboration Security** aproveitam nossa plataforma Nexus™ AI, que utiliza uma abordagem em várias camadas para detecção de ameaças.

## IA para detectar e bloquear ameaças

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 relacionamentos, inteligência sobre ameaças e modelos de linguagem para detectar e bloquear ataques com precisão.

**Os modelos de IA do Proofpoint Nexus processam 2,3 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 individuais e mais de 8.400 campanhas de ameaças ativas.**




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

O **Proofpoint 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 o risco de ataques associados ao comportamento.

**O Proofpoint 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 a emulação em área restrita para URLs e anexos suspeitos.

O **Proofpoint 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 Proofpoint Nexus ML™ (Machine Learning Model)** 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 soluções 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 da organização ou fora dela.

O **Proofpoint 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 Proofpoint Nexus RG™ (Relationship Graph)** compreende os relacionamntos para evitar perda acidental ou intencional de dados por e-mails endereçados incorretamente e cenários de vazamento de dados.

**O Proofpoint Nexus TI™ (Threat Intelligence)** protege contra contas comprometidas que enviam e-mails de phishing, tanto internamente quanto externamente.

**O Proofpoint Nexus CV™ (Computer Vision)** detecta conteúdo confidencial em imagens dentro de e-mails e documentos.

**O Proofpoint 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.

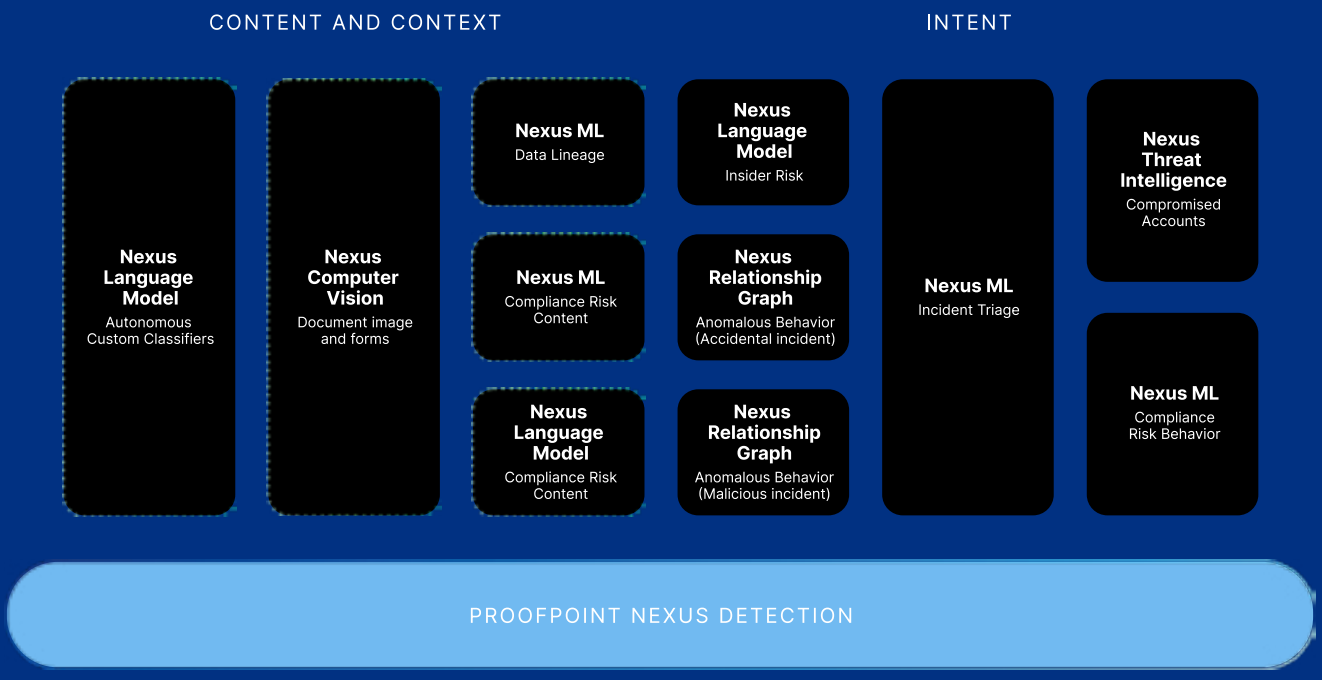



**Figura 1.** O Proofpoint Nexus impulsiona soluções de segurança e governança de dados.

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

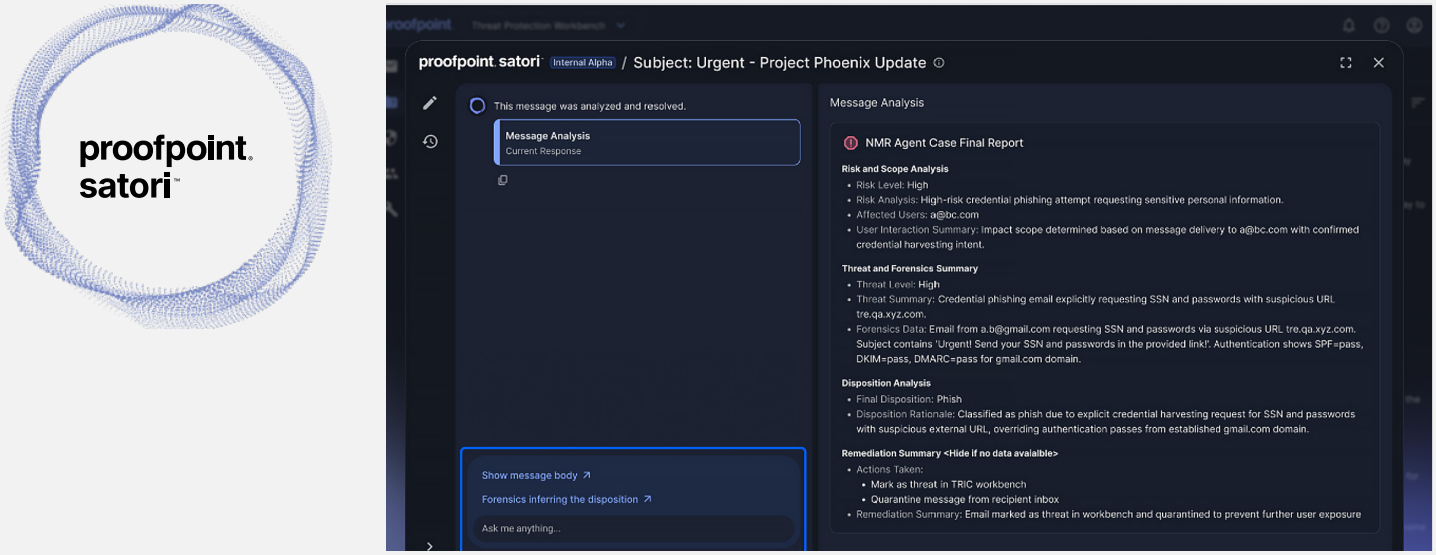



**Figura 2.** O Proofpoint Satori Abuse Mailbox Agent em ação.

## 2. Proofpoint Secure Agent Gateway

Entendemos as lacunas de segurança inerentes que surgem na implementação de fluxos de trabalho de IA agêntica dentro da sua organização. Portanto, estamos ampliando nossa plataforma Human-Centric Security para também proteger todos os seus agentes.

**O Proofpoint Secure Agent Gateway** protege os fluxos de trabalho agênticos existentes e unifica os controles sobre todos os agentes do seu ambiente.

- **Protege informações confidenciais** que fluem para dentro e para fora de cada fluxo de trabalho agêntico
- **Alimentado por nossa tecnologia MCP** (Model Context Protocol)
- **Controla o acesso a dados confidenciais** utilizados por agentes

Sobre a Proofpoint, Inc. A Proofpoint, Inc. é líder global em cibersegurança centrada em pessoas e agentes, protegendo a forma como pessoas, dados e agentes de IA se conectam por e-mail, nuvem e ferramentas de colaboração. A Proofpoint é uma parceira confiável de mais de 80 das empresas da Fortune 100, mais de 10.000 grandes empresas e milhões de organizações menores na contenção de ameaças, prevenção de perda de dados e construção de resiliência entre pessoas e fluxos de trabalho de IA. A plataforma de segurança de colaboração e de dados da Proofpoint ajuda organizações de todos os tamanhos a proteger e capacitar suas equipes para que possam adotar a IA de forma segura e confiante. Saiba mais em www.proofpoint.com/br

**Conecte-se à Proofpoint:** LinkedIn