

Proofpoint Data Security for AI

Monitore e controle o uso de dados confidenciais em aplicativos de IA autorizados e não autorizados

Principais vantagens

- Reduza o risco de dados impulsionado por IA
- Melhore a visibilidade sobre a atividade de IA na empresa
- Monitore e governe o uso de IA não autorizada
- Proteja dados confidenciais em prompts e uploads
- Acelere a adoção segura da IA
- Mantenha a conformidade e a prontidão para auditorias

O desafio: exposição de dados impulsionada por IA

Os aplicativos de IA generativa (GenAI) estão transformando as empresas, ajudando os funcionários a trabalhar mais rapidamente e de forma mais eficiente. Porém, as organizações também estão tendo dificuldades para governar como os dados confidenciais são compartilhados com ferramentas de IA, copilotos e aplicativos impulsionados por IA.

Os funcionários frequentemente fazem upload de arquivos e submetem prompts contendo informações confidenciais da empresa em ferramentas de IA autorizadas e não autorizadas. As tecnologias tradicionais de segurança de dados não foram projetadas para monitorar prompts de IA, uploads e respostas em tempo real. Isso deixa as organizações com visibilidade limitada sobre como os sistemas de IA acessam e expõem dados confidenciais.

Elementos internos também podem se aproveitar de ferramentas de IA — intencionalmente ou não — para encontrar, resumir, reescrever ou vaziar informações confidenciais, inclusive documentos confidenciais, propriedade intelectual e código-fonte pertencente à empresa. Elementos internos maliciosos podem usar IA para acelerar o roubo de dados, evadir controles tradicionais ou automatizar a extração de dados confidenciais em grande escala.

Sem os controles adequados, as organizações correm riscos de vazamento de dados, violações de conformidade e exposição não autorizada de informações reguladas ou confidenciais. As equipes de segurança precisam de visibilidade contínua sobre o uso e a exposição de dados por IA, imposição mais rigorosa de políticas e auditoria abrangente para respaldar uma adoção segura de IA.

A solução: Proofpoint Data Security for AI

A Proofpoint ajuda as organizações a adotar a IA de forma segura, com visibilidade sobre o uso de dados em IA autorizada e não autorizada. Ela unifica monitoramento, controles de dados específicos de IA e insights de atividade para reduzir riscos e permitir uma adoção de IA segura e escalável.

Capacidades críticas

Visibilidade sobre o uso de dados de IA e a postura de aplicativos de IA

A Proofpoint oferece visibilidade sobre como os funcionários e a IA interagem com os dados da empresa. As equipes de segurança podem identificar usuários de alto risco, detectar interações inseguras com IA e entender quais dados e documentos confidenciais estão expostos através do uso de IA autorizada e não autorizada.

Os classificadores personalizados autônomos da solução identificam dados confidenciais específicos da organização compartilhados através de prompts de IA, uploads e respostas geradas, inclusive propriedade intelectual, código-fonte, dados financeiros e documentos estratégicos. Esse contexto possibilita detecção, ocultação e proteção mais precisas em aplicativos de IA autorizados e não autorizados.

A Proofpoint monitora continuamente ambientes de IA e de software como serviço (SaaS) em busca de configurações incorretas, permissões excessivas em nível de site e integrações inseguras. Ao descobrir direitos de acesso excessivos e pontos fracos em configurações, as organizações podem remediar riscos, reduzir sua superfície de ataque e evitar que dados confidenciais sejam expostos a usuários e aplicativos de IA.

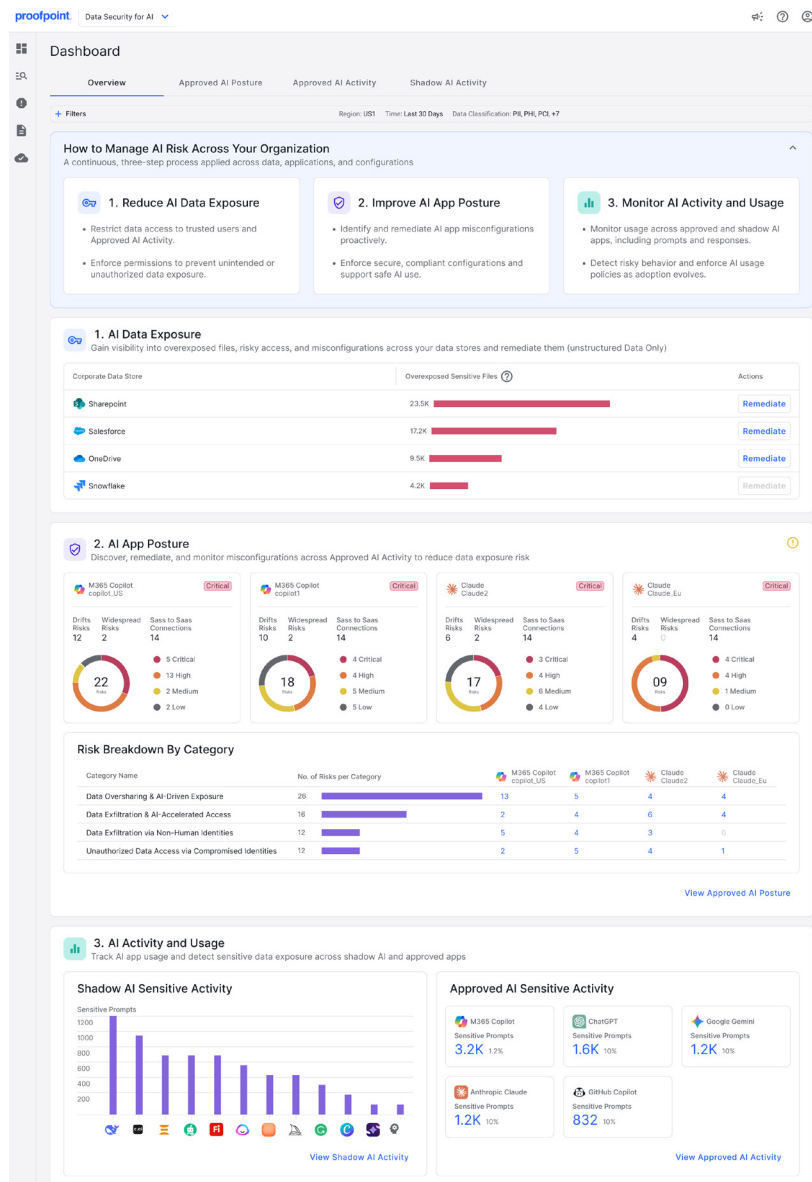


Figura 1. A Proofpoint oferece às equipes de segurança uma visão profunda de como os funcionários e as ferramentas de IA interagem com dados confidenciais.

Monitoramento e remediação de IA autorizada

A Proofpoint monitora continuamente prompts, uploads e respostas geradas por IA dentro de aplicativos de IA autorizados para identificar exposição de dados confidenciais e atividade interna incomum. Isso inclui atividade excessiva de prompts ou uploads em alto volume. A captura completa de prompts e respostas apoia investigações e prontidão para auditorias. Fluxos de trabalho de remediação integrados ajudam administradores e proprietários de arquivos a resolver rapidamente dados compartilhados em excesso.

Segurança de dados em IA não autorizada

As organizações podem reduzir a exposição de dados impulsionada por IA monitorando e controlando o uso de dados em aplicativos de IA não autorizados na Web e no desktop. A Proofpoint ajuda a prevenir a perda de dados em prompts, uploads e ações de colar. Ela também mascara dados confidenciais em prompts antes que sejam compartilhados com ferramentas de IA. Isso ajuda as organizações a escalar a adoção de IA de forma segura, sem bloquear completamente os aplicativos de IA.

Impacto operacional

Redução da perda de dados impulsionada por IA

Ajude a evitar a exposição de dados confidenciais em aplicativos de IA autorizados e não autorizados.

Melhoria na visibilidade e governança de IA

Obtenha visibilidade centralizada de como os funcionários e as ferramentas de IA interagem com os dados da empresa.

Adoção de uma IA empresarial mais segura

Viabilize o uso produtivo da IA generativa enquanto mantém controles de segurança, governança e conformidade.

Investigações e respostas mais rápidas

Capture a atividade de IA, prompts e respostas para apoiar investigações, remediação e prontidão para auditorias.

Postura de conformidade mais forte

Apoie a evolução dos requisitos de IA, privacidade e proteção de dados, aplicando políticas para informações reguladas, confidenciais e de propriedade da empresa usadas com ferramentas de IA.

Redução do risco de IA não autorizada

Descubra e governe o uso de IA não autorizada e comportamentos arriscados dos usuários enquanto minimiza impactos na produtividade da empresa.

Saiba mais

Para obter mais informações, visite [proofpoint.com/br](https://www.proofpoint.com/br).

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 empresas da Fortune 100, mais de 10.000 grandes corporações e milhões de organizações menores, ajudando a combater ameaças, prevenir perda de dados e desenvolver resiliência, tanto de pessoas quanto de 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 com a Proofpoint: [LinkedIn](#)

Proofpoint é uma marca registrada ou marca comercial da Proofpoint, Inc. nos Estados Unidos e/ou em outros países. Todas as demais marcas comerciais contidas neste documento são propriedade de seus respectivos donos.