

safetica

Proteção de IA

Proteja dados confidenciais sem impedir o uso produtivo da IA

A IA generativa está transformando a forma como os colaboradores trabalham, ao mesmo tempo que cria novos caminhos de risco para a exposição de dados confidenciais. À medida que aumenta o uso de ferramentas de IA, tanto aprovadas quanto não autorizadas, as equipes de segurança precisam de visibilidade que vá além de saber quais ferramentas estão sendo utilizadas. Elas precisam entender quem está usando IA, quais dados confidenciais estão sendo compartilhados e onde é necessária proteção adicional, sem restringir os benefícios de produtividade proporcionados pela IA.

Mantenha o controle sem bloquear o acesso às ferramentas de IA

Safetica AI Protection oferece visibilidade sobre a atividade de IA e o compartilhamento de dados confidenciais, com controles granulares que protegem os dados e, ao mesmo tempo, permitem que os colaboradores utilizem a IA de forma produtiva.

Com a Safetica, as equipes de segurança podem:



Identificar o uso de ferramentas de IA

aprovadas e não autorizadas em toda a organização para entender quais aplicativos os colaboradores estão utilizando.



Visualizar dados confidenciais em contexto

incluindo quem os está compartilhando, para onde estão sendo enviados e como estão sendo utilizados.



Proteger os dados antes que cheguem à IA

com políticas de DLP, controlando arquivos confidenciais, conteúdo colado, prompts e ações de usuários que apresentem riscos.



Aplicar controles granulares

com base no aplicativo de IA, na sensibilidade dos dados, no colaborador, no departamento e na atividade.



Investigar riscos relacionados à IA com mais contexto

e determinar a resposta adequada, em vez de bloquear completamente o acesso à IA.

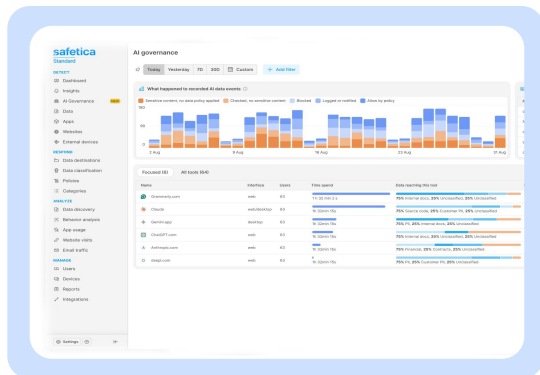
Governe o uso da IA. Proteja dados confidenciais.

A Safetica oferece uma proteção de IA em múltiplas camadas, combinando visibilidade sobre o uso da IA na organização com os controles de que as equipes de segurança precisam para proteger dados confidenciais contra exposição e gerenciar riscos sem prejudicar a adoção produtiva da IA.

Governança de IA

Obtenha visibilidade e controle à medida que os colaboradores aumentam o uso da IA

O Safetica AI Governance ajuda as equipes de segurança a entender e governar o uso de ferramentas de IA, tanto aprovadas quanto não autorizadas, oferecendo visibilidade sobre os aplicativos que os colaboradores utilizam, os dados que compartilham e onde aplicar controles. Você pode:

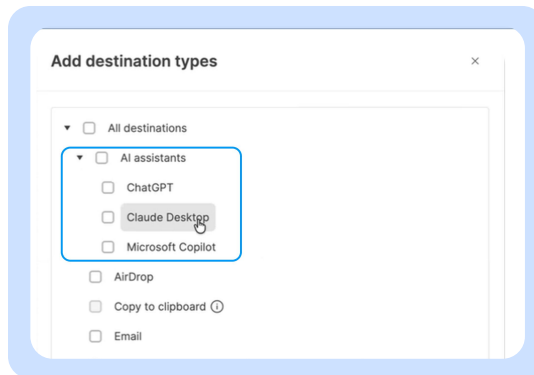


- **Conhecer seu ambiente de IA.** Mantenha uma visão centralizada dos aplicativos de IA aprovados e não autorizados em toda a organização.
- **Entender a atividade de IA.** Veja quem utiliza IA, com que frequência os aplicativos são acessados, quais dados e arquivos são compartilhados e qual proteção está atualmente implementada.
- **Transformar visibilidade em controle.** Monitore atividades, restrinja o compartilhamento de dados confidenciais, limite o acesso de usuários ou grupos específicos ou bloqueie completamente ferramentas que apresentem riscos.
- **Investigar com contexto.** Utilize prompts integrados e orientados por IA para explorar o uso e os riscos, resumir as conclusões e identificar ações que possam reforçar a proteção.

Políticas de dados para assistentes de IA

Proteja dados confidenciais antes que cheguem à IA

A Safetica estende a proteção de DLP aos assistentes de IA mais utilizados, ajudando as equipes de segurança a controlar informações confidenciais compartilhadas por meio de arquivos anexados, conteúdo copiado e colado e prompts, ao mesmo tempo que permite o uso adequado da IA. As equipes de segurança podem:



- **Proteger dados confidenciais antes que cheguem às ferramentas de IA.** Aplique políticas de DLP para monitorar e controlar arquivos confidenciais anexados, texto colado, prompts e outros dados compartilhados com ChatGPT, Claude e Microsoft Copilot.
- **Aplicar controles com base no contexto.** Defina políticas de acordo com a sensibilidade dos dados, a ferramenta de IA, o colaborador, o departamento e a ação específica do usuário, em vez de bloquear completamente o acesso à IA.
- **Proteger os dados durante o uso de aplicativos e navegadores.** Mantenha a proteção nos aplicativos de desktop compatíveis e em experiências de navegação baseadas em Chromium no macOS e Windows.
- **Permitir a continuidade do uso produtivo da IA.** Restrinja ações de compartilhamento de dados que apresentem riscos sem bloquear desnecessariamente o acesso produtivo às ferramentas de IA aprovadas.

Com a Safetica, você obtém a visibilidade necessária para entender o uso da IA, o contexto para identificar riscos reais e o controle para proteger dados confidenciais.