CLOUDFLARE

VISÃO GERAL DA SOLUÇÃO

Descubra o uso de IA não autorizada e TI invisível pela força de trabalho

Amplie a visibilidade sobre ferramentas não autorizadas de IA e SaaS com a inspeção de tráfego da Cloudflare

Revelar o que está oculto

A TI invisível não é um problema novo, mas a rápida adoção de ferramentas de IA não aprovadas está causando uma crise moderna:

- **20%** das organizações sofreram uma violação devido a incidentes de segurança com IA não autorizada em 2025[1]
- **85%** dos líderes de TI dizem que os funcionários estão adotando ferramentas de IA antes que a TI possa avaliá-las[2]

A Cloudflare restaura a visibilidade para as organizações gerenciarem essa superfície de ataque em expansão:

- **Analise o status do aplicativo:** categorize aplicativos de IA e SaaS como aprovados, não aprovados ou ainda em análise
- **Imponha políticas com base no status do aplicativo:** permita, bloqueie, isole, aplique detecções de DLP a interações, restrinja uploads de arquivos e muito mais
- **Analise o uso de aplicativos:** monitore tendências agregadas e realize investigações granulares
- **Avalie o risco de aplicativos:** avalie a confiabilidade por meio de pontuações de confiança de aplicativos

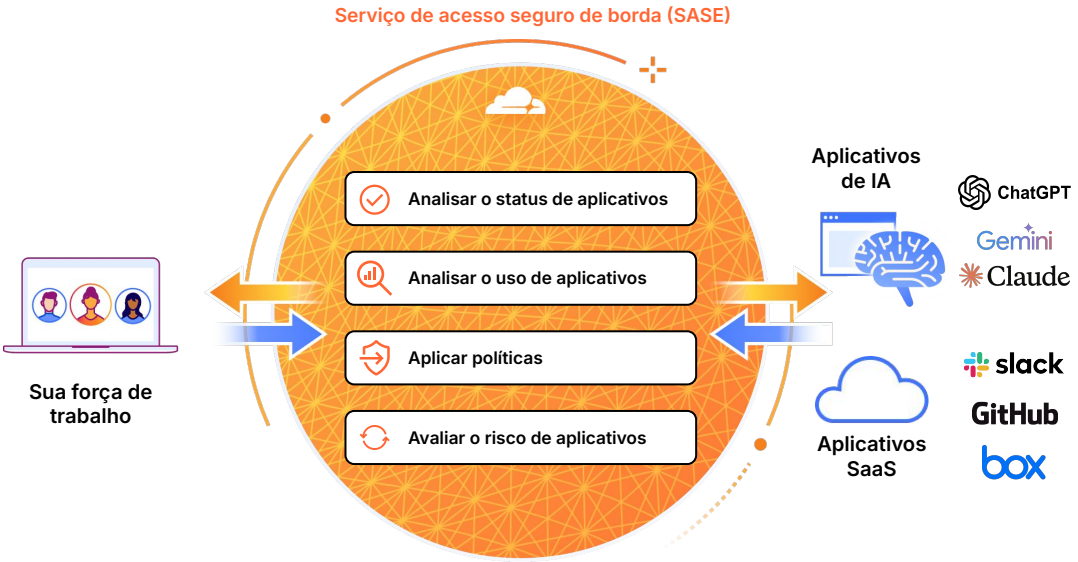
Riscos únicos da IA não autorizada

A IA não autorizada é diferente da TI invisível tradicional. Enquanto os aplicativos SaaS armazenam ou compartilham principalmente arquivos, as ferramentas de IA transformam e aprendem com qualquer entrada de funcionário.

Isso significa que o IP, os dados de clientes ou o código-fonte confidenciais podem ser absorvidos de forma irreversível para o treinamento de modelos, sem possibilidade de remoção.

Como funciona

A plataforma SASE da Cloudflare fica em linha entre sua força de trabalho e os recursos para unificar a visibilidade e os controles.



Além disso, integre o CASB da Cloudflare por meio da API para verificar configurações incorretas, atividades de usuários e dados confidenciais. Gerencie a postura de segurança em aplicativos de IA (ChatGPT, Claude, Google Gemini) e outros aplicativos SaaS. Use o CASB com seu provedor de identidade para ver quando os usuários são autenticados em aplicativos de terceiros não autorizados.

Exemplo de painéis

Filtre essa visão geral de alto nível do uso de aplicativos com base em:

- Aplicativo e tipo de aplicativo
- Status de aprovação
- Proteção por ZTNA
- Número de usuários

Para mais detalhes, clique no nome de qualquer aplicativo de IA para ver usuários ou grupos específicos que o acessam, sua frequência de uso, local e a quantidade de dados transferidos.

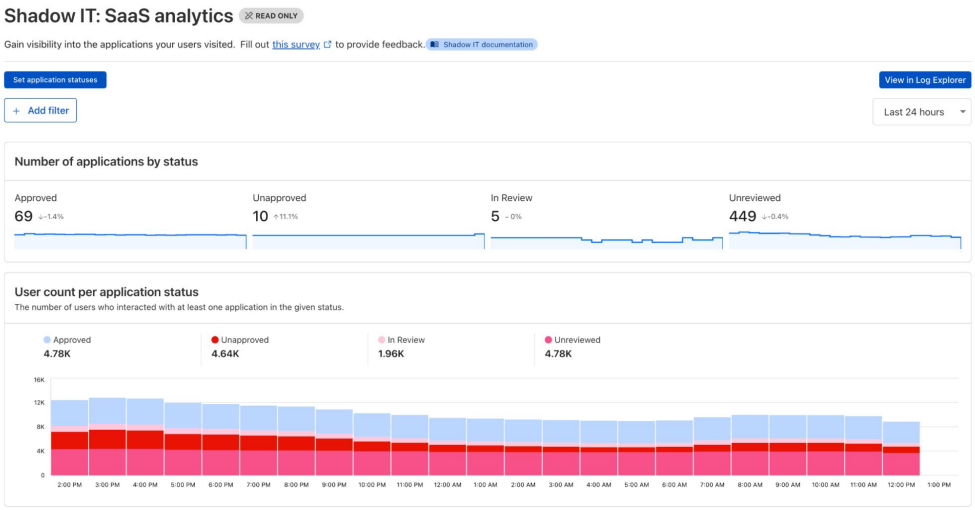


Figura 1: Painel de análise de dados de TI Invisível

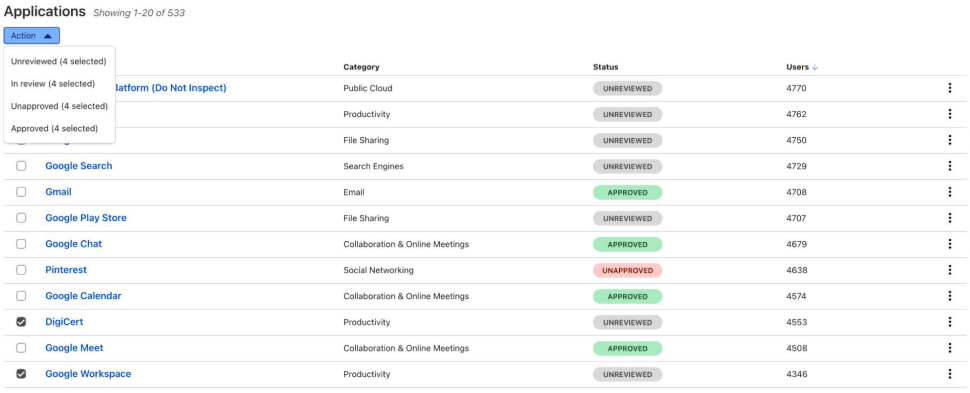


Figura 2: Marcar os status dos aplicativos

Organize aplicativos e defina políticas de acesso com base no status de aprovação:

- Aprovado (autorizado)
- Reprovado (não autorizado)
- Em análise
- Não analisado

Quer mais orientação técnica? Saiba como criar políticas com este caminho de aprendizagem.

Quer se aprofundar em como proteger sua adoção de IA?

Explore mais casos de uso | **Solicite um workshop**

1. Relatório IBM, Cost of a Data Breach de 2025: Fonte
2. 2025 Manage Engine research: Fonte