CLOUDFLARE

RESUMO DO PRODUTO

Agente de segurança de acesso à nuvem

Visibilidade e controle abrangentes sobre ambientes SaaS, de IA e em nuvem, protegendo os dados sem desacelerar a inovação.

Segurança SaaS desenvolvida para a era da IA

Proteja seus ambientes SaaS, de IA e em nuvem sem diminuir a produtividade. Detecte configurações incorretas, TI invisível e riscos de dados instantaneamente em sua força de trabalho híbrida usando o Cloudflare CASB.

- **Automatize a conformidade:** detecte e corrija instantaneamente lacunas de segurança, como compartilhamento de arquivos não autorizado ou MFA fraco, no Microsoft 365, Google Workspace e GitHub.
- **Detenha IA não autorizada/TI invisível:** descubra aplicativos não autorizados e bloqueie o acesso a armazenamento em nuvem ou sites de compartilhamento de arquivos não aprovados.
- **Uso seguro de IA:** obtenha visibilidade da adoção de ferramentas de IA e imponha restrições de locatários em plataformas como ChatGPT e Gemini para garantir acesso somente corporativo.
- **Gerencie riscos de terceiros:** identifique e revogue integrações de terceiros arriscadas que têm acesso a seus dados corporativos.

Construída em nossa rede global, a proteção in-line e orientada por API do Cloudflare CASB garante segurança rápida e econômica em escala.

EESTI RAUDTEE

Provedor de infraestrutura

Vulnerabilidades de SaaS identificadas — como arquivos sensíveis do SharePoint sendo amplamente compartilhados — para ajudar a mitigar a perda de dados.

Leia o estudo de caso

APPLIED

Provedor de software de seguros

Protegeu a adoção da IA generativa bloqueando entradas de dados sensíveis em ferramentas como o ChatGPT sem prejudicar a produtividade da força de trabalho.

Leia o estudo de caso

Provedor de telessaúde

Dados sensíveis de pacientes protegidos (PHI/HIPAA) e acesso acelerado para uma força de trabalho remota em rápido crescimento usando DLP e CASB.

A diferença da Cloudflare

Implantação instantânea e sem cliente

Conecte-se a aplicativos SaaS e de IA como Microsoft 365, GitHub, Slack e ChatGPT em minutos via API. Verifique imediatamente riscos históricos, configurações incorretas e exposição de dados sem instalar clientes.

Gerenciamento contínuo de SaaS e postura de dados em nuvem

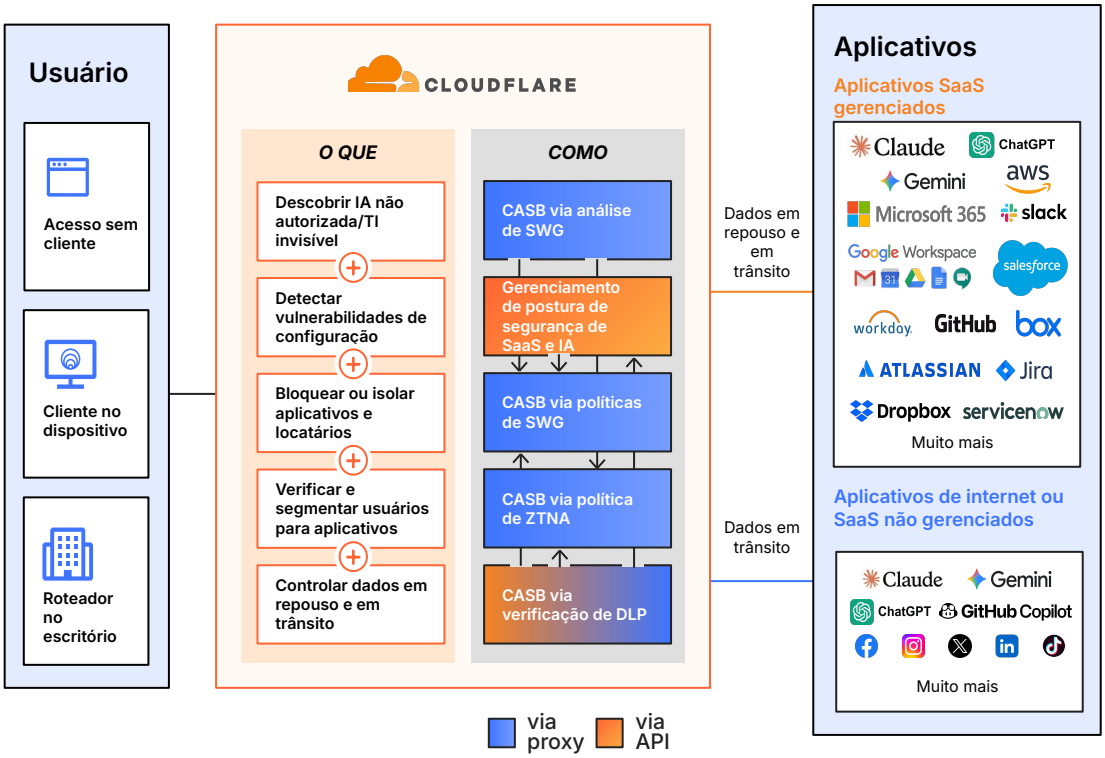
Identifique desvios de segurança e configurações inseguras no seu SaaS e no seu armazenamento em nuvem. Detecte e reverta configurações incorretas críticas, como buckets S3 públicos ou permissões de projetos abertos, antes que levem a uma violação.

Controle unificado de TI Invisível

Pare de ficar alternando entre consoles. Use insights do CASB para detectar aplicativos não aprovados e, em seguida, acione instantaneamente as políticas Zero Trust para bloquear ou isolar esse tráfego por meio do Cloudflare Gateway, gerenciando tudo a partir de um único painel.

Quer se aprofundar neste produto? Analise nossa arquitetura de referência ou fale com um especialista.

Segurança abrangente para SaaS, IA e TI invisível



Como funciona

O CASB multimodo da Cloudflare ajuda a fornecer segurança em nuvem unificada para aplicativos SaaS. Para proteger os dados em repouso, integrações de APIs simples verificam continuamente seus aplicativos em busca de vulnerabilidades e possíveis riscos.

Nossos controles de acesso Zero Trust (ZTNA), gateway (SWG) e isolamento do navegador (RBI) são implantados perfeitamente como um CASB in-line, combinando configuração fácil com segurança robusta.

Proteção de dados fora de banda e postura de segurança SaaS (orientada por API)	
Gerenciamento de postura de segurança SaaS (SSPM)	Analise aplicativos SaaS e armazenamento em nuvem via API para detectar configurações incorretas e integrações de terceiros arriscadas (por exemplo, buckets S3 públicos, aplicativos OAuth não autorizados ou violações de MFA).
Proteção de dados SaaS (DLP)	Detecte arquivos confidenciais (PCI, informações de identificação pessoal, segredos) usando a verificação de dados em repouso e corrija as violações automaticamente (por exemplo, remover arquivos acessíveis publicamente) para impor a conformidade.
Proteção de dados in-line (orientada por proxy)	
Descoberta de IA não autorizada e TI invisível	Visibilidade instantânea do uso de aplicativos não autorizados. Categorize e bloqueie/isole automaticamente aplicativos arriscados (por exemplo, conversores de PDF ou ferramentas de IA não aprovados) com base nas pontuações de confiança de aplicativos.
DLP e OCR in-line	Detecte dados confidenciais no tráfego usando Correspondência exata dos dados (EDM) e classificadores avançados. Aproveite o reconhecimento óptico de caracteres (OCR) para estender essas proteções às imagens, bloqueando o vazamento de dados.
Proteção para prompts de GenAI	Evite que dados sensíveis (código-fonte, informações de identificação pessoal de clientes) sejam colados em LLMs públicos. Inspecione solicitações HTTPS para ferramentas como ChatGPT ou Gemini para aplicar o uso seguro de IA.
Controle de locatários	Implemente acesso somente corporativo para aplicativos como Microsoft 365, Google Workspace e Slack para evitar logins de contas pessoais em dispositivos corporativos.
Gerenciamento unificado	
Cliente único	Não é necessário um cliente CASB separado. O cliente unificado lida com ZTNA, SWG e CASB com inspeção de passagem única.
Pontuação de risco de usuários	Detecte usuários comprometidos correlacionando descobertas do CASB com anomalias comportamentais para atribuir pontuações de risco dinâmicas.
Logpush	Registro de logs abrangente captura todas as solicitações, usuários e dispositivos. Exporte instantaneamente logs do CASB para Splunk, Datadog ou S3 para análise SIEM.

© 2026 Cloudflare, Inc. Todos os direitos reservados.