CLOUDFLARE

RESUMO DA SOLUÇÃO

Proteger seus dados confidenciais

Melhor arquitetura de rede para proteção de dados mais eficaz, mais produtiva e mais ágil.

Proteção unificada para dados em qualquer lugar

A proteção de dados não é uma exigência nova. No entanto, a mudança para arquiteturas de nuvem híbrida, juntamente com a rápida adoção da IA, apresenta novos desafios:

- **93% dos funcionários** admitem inserir informações em ferramentas de IA sem aprovação [1]
- **79% de todos os países** têm legislações sobre privacidade de dados [2]

A Cloudflare impõe controles consistentes em todo o ciclo de vida dos seus dados:

- **Proteja em todos os lugares:** aplique controles consistentes no tráfego da web, SaaS, e-mail e nuvem.
- **Bloqueie a exfiltração de IA:** analise os prompts de IA generativa para bloquear dados sensíveis e gerenciar o uso de IA.
- **Gerencie os riscos de dados:** descubra e administre a TI invisível/IA não autorizada e analise aplicativos SaaS/em nuvem com o CASB.

"O aumento de todas essas ferramentas de IA não autorizadas nos faz reconsiderar nossa abordagem de segurança. Estamos analisando o SASE agora." — *Head of Infosec,* ***AllSaints***

Por que usar o SASE em vez do DLP corporativo?

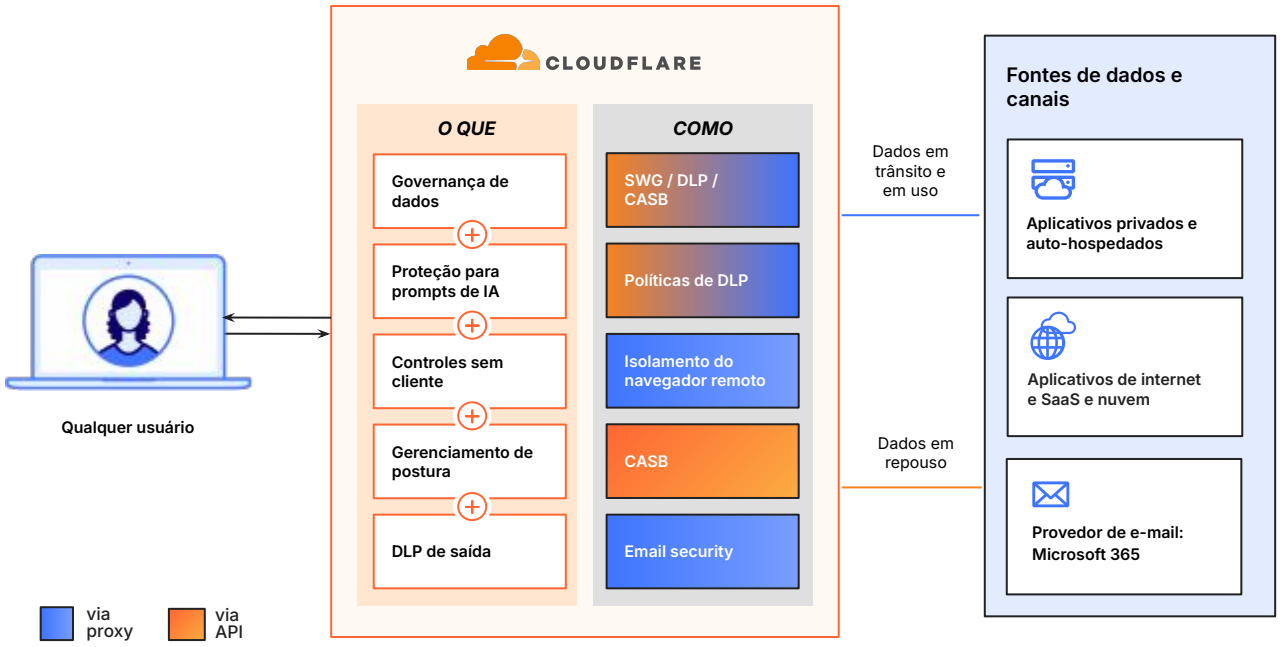
A plataforma de serviço de acesso seguro de borda (SASE) da Cloudflare foi construída para ficar entre sua força de trabalho e todos os aplicativos e fontes de dados. Isso faz do SASE um ponto de partida ideal para começar a proteger dados com segurança.

Seja acessando dados em aplicativos de SaaS, baixando arquivos sensíveis ou conversando com ferramentas de IA generativa, a plataforma SASE da Cloudflare impõe controles de segurança consistentes em todas as interações de dados.

Como funciona

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

Proteção de dados com tecnologia de IA com a plataforma de SASE da Cloudflare em tráfego da web, SaaS, e-mail e nuvem



Proteção de dados in-line em tempo real

- **DLP granular:** acabe com a exposição de dados sensíveis com detecções contextuais para informações de identificação pessoal, código-fonte, dados de clientes e muito mais.
- **DLP para e-mails enviados:** detecte automaticamente dados sensíveis em e-mails de saída, prevenindo vazamentos acidentais de informações.
- **Proteção para prompts:** detecte e bloqueie prompts e respostas de IA arriscados com base na intenção (por exemplo, tentativas de jailbreak, violação de código, solicitações de informações de identificação pessoal).

Acesso seguro e controles do cliente

- **Acesso seguro a aplicativos:** aplique regras de acesso à rede Zero Trust (ZTNA), como a verificação granular de DLP para conexões de IA agêntica, em todos os aplicativos corporativos.
- **Verificações de postura do dispositivo:** controle o acesso com base em verificações granulares de postura, como criptografia de disco e DLP de endpoint habilitado.
- **Controles sem cliente:** aplique controles de dados baseados em navegador para proteger o acesso de terceiros e as políticas de BYOD dos funcionários.

TI invisível e riscos de postura

- **Descoberta de IA não autorizada e TI invisível:** descubra e gerencie IA não autorizada e TI invisível em todo o seu ambiente. Quantifique o risco com pontuações de confiança de aplicativos e métricas de transferência de dados para mitigar rapidamente a exposição.
- **Gerenciamento de postura:** analise aplicativos de SaaS e ambientes em nuvem em busca de riscos relacionados à postura. Adote medidas prescritivas para remediar as falhas de segurança.
- **Controle de locatários:** bloqueie locatários pessoais de aplicativos de SaaS para evitar a exfiltração de dados.

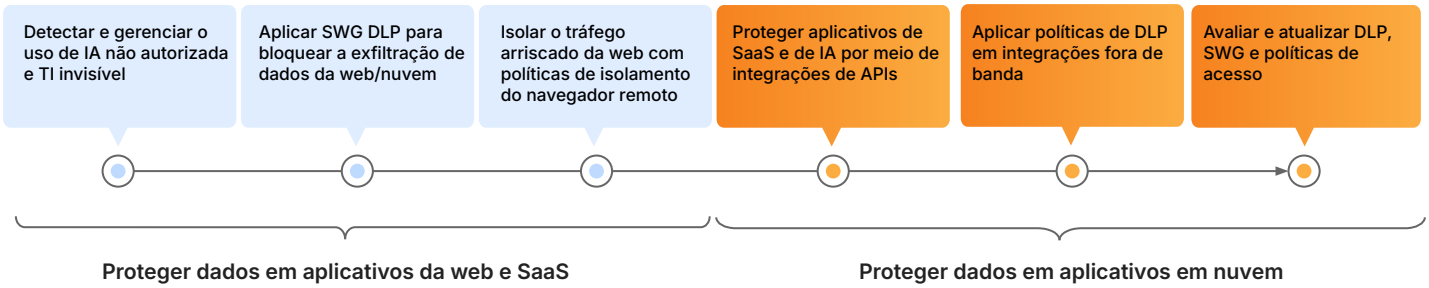
Integrações e relatórios

- **Integrações com CASB:** integre-se perfeitamente às principais plataformas de SaaS e de IA (incluindo Microsoft 365, Google Workspace e ChatGPT) para varreduras de CASB baseadas em API.
- **Integração com Microsoft MIP:** sincronize continuamente com rótulos do Microsoft Information Protection (MIP) para políticas de DLP consistentes.
- **Observabilidade e computação forense**: registre dados com segurança no seu SIEM preferido para auditoria ou analise logs instantaneamente por meio do painel ou da API.

Exemplo de jornada de proteção de dados

Comece descobrindo o uso de IA não autorizada e TI invisível para aumentar a visibilidade da superfície de ataque. Configure políticas fundamentais de DLP no SWG para bloquear o vazamento de dados de alto risco de aplicativos em nuvem não gerenciados, além de implementar o isolamento do navegador remoto para tráfego da web não aprovado.

Em seguida, implante o CASB para proteger aplicativos de SaaS e de IA autorizados, corrigindo configurações incorretas e aplicando políticas de compartilhamento interno. Refine e integre políticas de DLP granular e de acesso no SWG, e-mail e CASB para alcançar uma prevenção automatizada e unificada em todos os principais vetores de dados.



Exemplos de casos de uso para começar

- **Bloquear a exfiltração em tempo real de informações de identificação pessoal/PHI** em todos os canais de comunicação e armazenamento não autorizados.
- **Proteger o código-fonte e a propriedade intelectual (IP)** contra roubo interno e distribuição não autorizada.
- **Aplicar políticas de proteção de prompts** para aplicativos de IA generativa para evitar a exposição de dados confidenciais e a contaminação de modelos.
- **Evitar configurações incorretas** e implementar controles de acesso granulares em todos os aplicativos de SaaS e de IA.

Resultados de clientes

EESTI RAUDTEE

Provedor de infraestrutura
Leia o estudo de caso

Mitigar a perda de dados e vulnerabilidades de SaaS

identificando vazamentos de dados e configurações incorretas.

APPLIED

Tecnologia para seguros
Leia o estudo de caso

Isolar ferramentas públicas de IA generativa como o ChatGPT

para bloquear a ação de copiar e colar dados sensíveis.

Flo

Aplicativo de saúde líder
Leia o estudo de caso

Proteger os dados dos pacientes

e alcançar a conformidade com segurança de e-mail e Zero Trust.

CREDIT SAISON INDIA

Mutuante NBFC
Leia o estudo de caso

Proteger as informações de identificação pessoal e garantir a conformidade

para evitar a saída indesejada de dados.

Quer conversar sobre suas necessidades de proteção de dados?

Solicite um workshop

1. 2025 Manage Engine research: Fonte
2. 2025 United Nations Conference on Trade & Development: Fonte