CLOUDFLARE

RESUMO DA SOLUÇÃO

Cloudflare One para proteção de dados

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

Proteção unificada para dados em qualquer lugar

Os riscos para os dados atuais exigem segurança moderna
Atualmente, os dados estão explodindo em volume, variedade e velocidade, e as organizações enfrentam riscos crescentes decorrentes de:

Amplos ambientes de nuvem e SaaS
↳ incluindo ferramentas de IA emergentes e opacas, como ChatGPT
↳ levando à exposição de código-fonte precioso

O pacote de proteção de dados do Cloudflare One foi desenvolvido para permanecer na vanguarda desses riscos claramente modernos.

Ao unificar soluções pontuais em uma única plataforma e rede, a Cloudflare oferece proteção de dados que é:

- **Mais eficaz** ao simplificar a conectividade e o gerenciamento de políticas
- **Mais produtivo** ao garantir experiências do usuário rápidas, confiáveis e consistentes em qualquer lugar
- **Mais ágil** ao inovar rapidamente para atender aos seus requisitos de segurança em constante evolução

Serviços de segurança na borda (SSE) do One para proteger os dados na web, no SaaS e em aplicativos privados

Adote progressivamente a Cloudflare em sua jornada de SSE para:

1. Acesso seguro aos dados com Zero Trust
2. Impedir ameaças como phishing e ransomware
3. Detectar e bloquear suas informações mais confidenciais

Navegue pelos crescentes riscos de dados...

Ampla presença de SaaS

82%

das violações envolveram dados armazenados em ambientes de nuvem.[1]

E, claro, os custos de violação de dados continuam aumentando, um aumento de 15% nos últimos 3 anos. [1]

Regulamentações novas e diferentes

71%

de todos os países têm legislação para proteger dados e privacidade.[2]

Nos EUA, **11 estados** agora têm leis abrangentes de proteção de dados – contra 3 em 2021[3]

Transformação digital

89%

dos CISOs afirmam que avançar rapidamente com iniciativas de transformação digital introduz riscos imprevistos na segurança dos dados da empresa[4]

Caso de uso nº 1: Proteger o código de desenvolvedores

Problema
O código pode ser exposto ou alvo de roubo em muitas ferramentas para desenvolvedores, inclusive em locais à vista, como repositórios públicos.

Solução
Procurar e corrigir repositórios públicos mal configurados, como o GitHub, que correm o risco de vazamento de código. Detectar o código-fonte em uploads / downloads e aplicar controles.

→ GitHub
→ GitLab
→ Bitbucket

Caso de uso nº 2: Visibilidade da exposição de dados e gerenciamento de riscos

→ OpenAI
→ Bard
→ GitHub Copilot

Problema
Os dados estão espalhados em diversos ambientes SaaS e de nuvem, TI invisível não sancionada e ferramentas emergentes de IA, como ChatGPT, criando mais risco de vazamentos.

Solução
Verifique se há configurações incorretas em suítes SaaS com detecções DLP integradas para dados confidenciais. Obtenha visibilidade do uso não autorizado de aplicativos e permita, bloqueie, isole ou aplique controles Zero Trust para acessá-los.

Caso de uso nº 3: Cumprir os regulamentos

Problema
Requisitos legais mais rigorosos e mais abrangentes para as empresas manterem os dados seguros e privados, com multas crescentes pelo não cumprimento.

Solução
Identificar e aplicar controles a classes de dados regulamentadas (PII, saúde, financeiro). Manter trilhas de auditoria detalhadas por meio de registros e análises adicionais do SIEM. Reduzir a superfície de ataque com uma postura de segurança Zero Trust abrangente.

- ✓ GDPR
- ✓ DPDP
- ✓ CCPA
- ✓ CPRA
- ✓ GLBA
- ✓ PCI DSS
- ✓ HIPAA
- ✓ ISO
- ✓ Muitos outros

Como funciona

Uma plataforma unificada

A Cloudflare converge visibilidade e controles de DLP, CASB, ZTNA, SWG, RBI e serviços de segurança de e-mail em uma única plataforma para um gerenciamento mais simples.

Uma rede programável

Um plano de controle com serviços criados em nossa própria plataforma para desenvolvedores para impor controles para dados em trânsito, em uso e em repouso em todos os pontos de aplicação: web, SaaS ou ambientes de aplicativos privados.

Exemplo de controles com serviços que podem ser compostos

Aplicar DLP para dados em trânsito e acesso seguro

- Analisar dados confidenciais em tráfego e arquivos e configurar políticas de bloqueio com DLP.
- Descobrir e gerenciar TI invisível com CASB.
- Acesso seguro aos dados em aplicativos com ZTNA.
- Bloquear locatários pessoais de aplicativos SaaS para evitar a exfiltração de dados.

Isolar aplicativos para proteger os dados em uso

- Bloquear copiar/colar, fazer upload / download, imprimir, entradas de teclado, tudo sem um dispositivo cliente.
- A implantação sem cliente é perfeita para dispositivos não gerenciados, usuários de terceiros e ferramentas de IA como ChatGPT.
- Aplicar políticas DLP em aplicativos isolados.

Proteger dados inativos em aplicativos SaaS

- Analisar aplicativos SaaS em busca de atividades suspeitas, configurações incorretas e dados confidenciais.
- Adotar medidas prescritivas para remediar riscos através de políticas de SWG.

Se integrar para agilizar a conformidade e os controles

- Logpush para seu SIEM preferido para correlação e auditoria.
- Se integrar com 18 dos pacotes SaaS mais populares para varreduras CASB baseadas em API.
- Sincronizar continuamente com rótulos de Proteção de Informações da Microsoft (MIP) para suas políticas DLP.

Melhor proteção de dados com a Cloudflare

Mais eficaz ***ao reduzir a complexidade***

Simplifique a conectividade com muitas opções flexíveis para enviar tráfego à Cloudflare para aplicação.

Use verificações baseadas em API para suítes SaaS ou modos sem cliente para ZTNA e RBI para proteger o acesso ao aplicativo. Para encaminhar o tráfego de proxy, use um cliente de dispositivo ou vias de acesso de rede de área ampla nos serviços de segurança.

Mais produtivo ***ao melhorar as experiências do usuário***

Nossa rede está em toda parte, garantindo que os controles sejam aplicados com inspeção de passagem única, próxima aos usuários finais e aos dados, onde quer que estejam.

Experiências do usuário final confiáveis e não invasivas significam que a aplicação de controles de dados nunca interrompe o trabalho.
Comprovadamente mais rápido que os outros SSE..

Mais ágil ***ao inovar com velocidade***

Nossa arquitetura de rede programável nos permite desenvolver recursos rapidamente, para que você possa se adaptar a novos riscos com agilidade.

Adotamos rapidamente novos padrões e protocolos de segurança (como conexões somente IPv6 ou criptografia HTTP/3) para que a proteção de dados permaneça atualizada.

O que os clientes dizem

"Hoje, o Cloudflare One ajuda a evitar que nossos usuários compartilhem dados e códigos confidenciais com ferramentas como ChatGPT e Bard, permitindo-nos aproveitar as vantagens da IA com segurança... No futuro, estamos entusiasmados com as inovações contínuas da Cloudflare para proteger os dados e, em particular, sua visão e roteiro para serviços como DLP e CASB."

Tanner Randolph
Diretor de segurança de informações, (CISO)

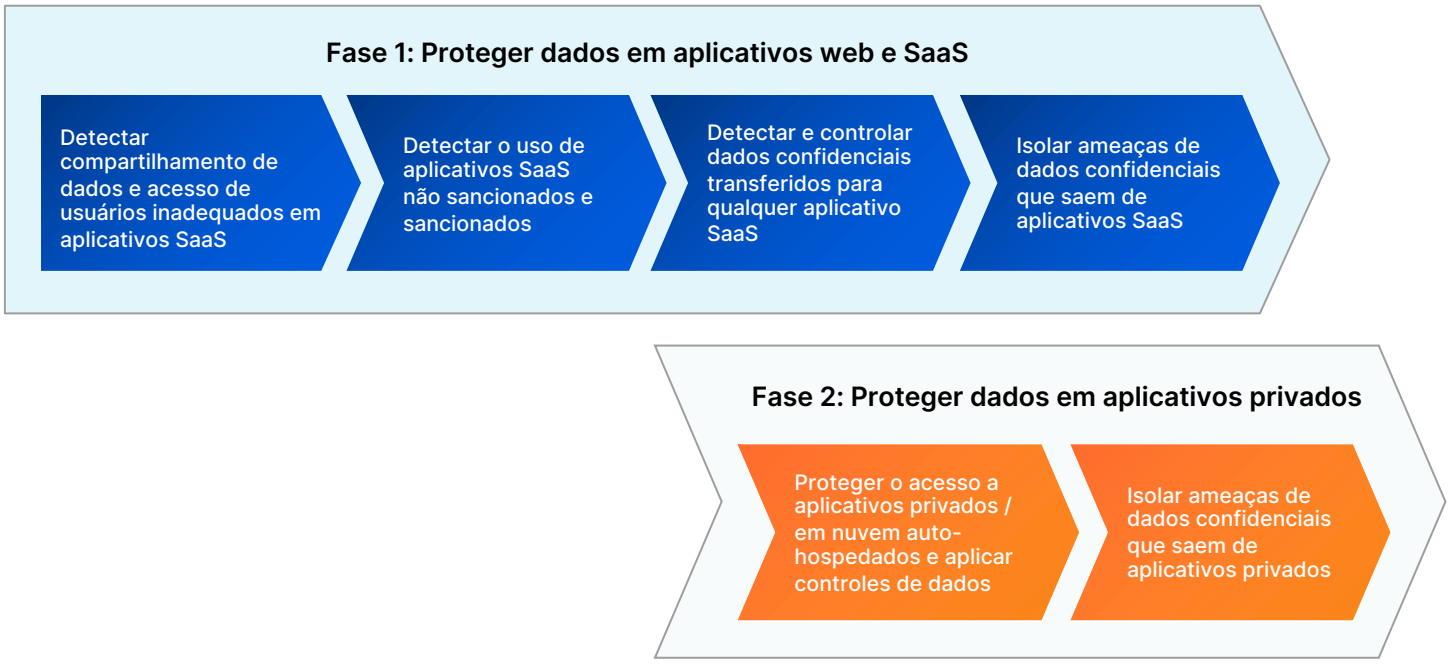
Applied Systems

Leia o estudo de caso

Outros casos de uso

- **Empresa de gás natural da Fortune 500** para proteger o acesso do prestador de serviços aos dados
- **Importante site de empregos dos EUA** para proteger código e informações pessoais
- **Companhia aérea regional dos EUA** para mitigar riscos de exposição de dados de clientes
- **Empresa australiana de saúde** para proteger dados médicos regulamentados
- **Fabricante de dispositivos médicos dos EUA** para simplificar a conformidade com a HIPAA

Caminhos comuns de adoção



Comece a usar

SAIBA MAIS...

sobre o aumento dos riscos de dados neste infográfico

INTERAJA...

com o funcionamento da plataforma nesta demonstração

EXPERIMENTE...

o valor solicitando um workshop consultivo

1. Cost of a Data Breach Report 2023, IBM
2. United Nations Conference on Trade & Development
3. International Association of Privacy Professionals (IAPP)
4. 2023 “State of the CISO” report