DLP e CASB integrados

O Cloudflare One melhora a visibilidade dos dados e reduz o risco de exfiltração à medida que os dados são transferidos pela web, SaaS e aplicativos auto-hospedados/privados.

Proteger dados em qualquer lugar

Cerca de 81% das violações agora envolvem dados armazenados em ambientes de nuvem.

Hoje, as organizações estão processando mais dados do que nunca. Os clientes confiam suas informações pessoais às empresas. Os trabalhadores do conhecimento modernos precisam aproveitar e compartilhar dados em ambientes de nuvem e SaaS para realizar seu trabalho. E o código agora tem um valor inestimável para uma empresa, crescendo rapidamente em volume todos os dias. Os dados confidenciais agora residem em todos os lugares.

Prevenção integrada de perda de dados (DLP) + Agente de segurança de acesso à nuvem (CASB) multimodo

Integrados em uma plataforma SSE combinável, o DLP e o CASB da Cloudflare ampliam facilmente a visibilidade e unificam os controles de proteção de dados em todos os aplicativos, usuários e dispositivos. A simplicidade e a flexibilidade de implantação para os administradores garantem que as políticas sejam funcionais, não estéreis.

75% De redução de custos (ou custos menores) associados ao uso de várias soluções pontuais [1]

69% De minimização do tempo gasto em tarefas de baixo valor (ou seja, instalação e configuração de políticas de defesa contra ameaças [1]

20% De redução da probabilidade e dos custos relacionados a uma violação de dados [2]

Adote os aplicativos SaaS e a nuvem com segurança

Evite multas regulatórias

Mitigue os danos financeiros e à reputação causados por violações de conformidade de dados com uma aplicação de políticas mais simplificada para dados regulamentados.

Simplifique a segurança SaaS

Capacite sua empresa a adotar novos aplicativos SaaS com segurança e confiança. Elimine os pontos cegos com detecção contínua e controle sobre os riscos de SaaS.

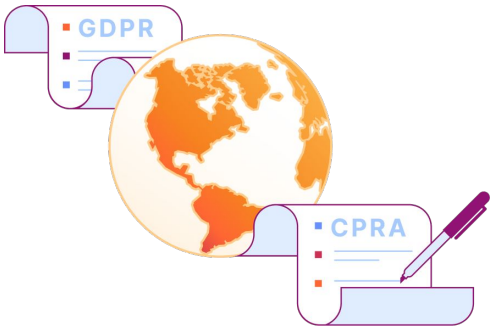
Escale no seu próprio ritmo

Proteja a segurança dos dados sem interromper as operações diárias. A configuração é simples e a experiência do usuário é perfeita.

Principais casos de uso para DLP e CASB

Simplificar a conformidade regulatória

Reduza o risco de violações de conformidade causadas por violações de dados com uma postura de segurança Zero Trust abrangente. O DLP identifica e aplica controles para classes de dados regulamentadas (informações de identificação pessoal, saúde, financeiros). Além disso, mantenha trilhas de auditoria de dados detalhadas por meio de logs e análises adicionais do SIEM para facilitar os esforços de conformidade.

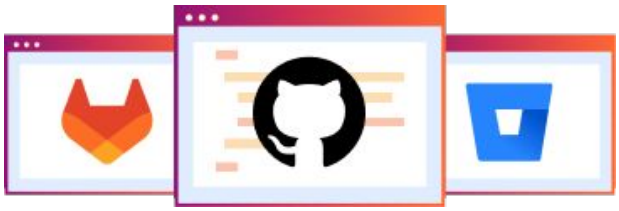


Aumente a visibilidade dos dados e dos riscos de configuração incorreta

Não é possível proteger o que você não conhece. O CASB da Cloudflare verifica suítes SaaS em busca de configurações incorretas e ameaças a dados com detecções de DLP integradas em busca de dados confidenciais. Obtenha rapidamente visibilidade do uso de aplicativos não autorizados, como ferramentas emergentes de IA, como ChatGPT e Bard. Em seguida, reduza os riscos permitindo, bloqueando, isolando ou aplicando controles Zero Trust para acessá-los.

Proteja a propriedade intelectual e códigos de desenvolvedores valiosos

O CASB detecta e corrige repositórios públicos mal configurados, como o GitHub, que correm o risco de vazamento de código. Para o código-fonte em trânsito, aplique controles DLP granulares para impedir que os usuários façam upload/download para qualquer aplicativo ou dispositivo.



Começar a usar a proteção de dados unificada

Seja mais proativo com sua proteção de dados com uma abordagem Zero Trust. Determine como os usuários corporativos estão usando aplicativos SaaS, web e privados e identifique de forma granular quais eles estão usando. Em seguida, aplique controles de dados e políticas orientadas por identidade/dispositivos para reduzir sua superfície de ataque.

Obter visibilidade sobre a movimentação de dados

- Detectar compartilhamento inadequado de dados confidenciais em aplicativos SaaS
- Detectar aplicativos SaaS não sancionados e sancionados
- Integrar logs com provedores SIEM para auditoria*

Reduzir o risco de exfiltração de dados

- Aplicar controles DLP para o que/para onde os dados são transferidos em qualquer aplicativo
- Isolar ameaças de dados que saem de aplicativos SaaS e privados*
- Proteger o acesso a aplicativos SaaS e auto-hospedados privados/em nuvem*

**usando recursos de ZTNA, SWG e isolamento do navegador remoto na plataforma SSE e SASE*

Como o DLP funciona

A migração para a nuvem tornou o rastreamento e o controle de informações confidenciais mais difíceis do que nunca. Os funcionários estão usando uma lista cada vez maior de ferramentas para manipular uma grande quantidade de dados. Enquanto isso, os gerentes de TI e de segurança lutam para identificar quem deve ter acesso a dados confidenciais, como esses dados são armazenados e para onde esses dados podem ir.

A prevenção contra perda de dados permite que você proteja seus dados com base em suas características, como palavras-chave ou padrões. À medida que o tráfego entra e sai da infraestrutura corporativa, o tráfego é inspecionado em busca de indicadores de dados confidenciais. Se os indicadores forem encontrados, o tráfego será permitido ou bloqueado com base nas regras do cliente.

Controles fáceis e rápidos sobre classes de dados regulamentadas

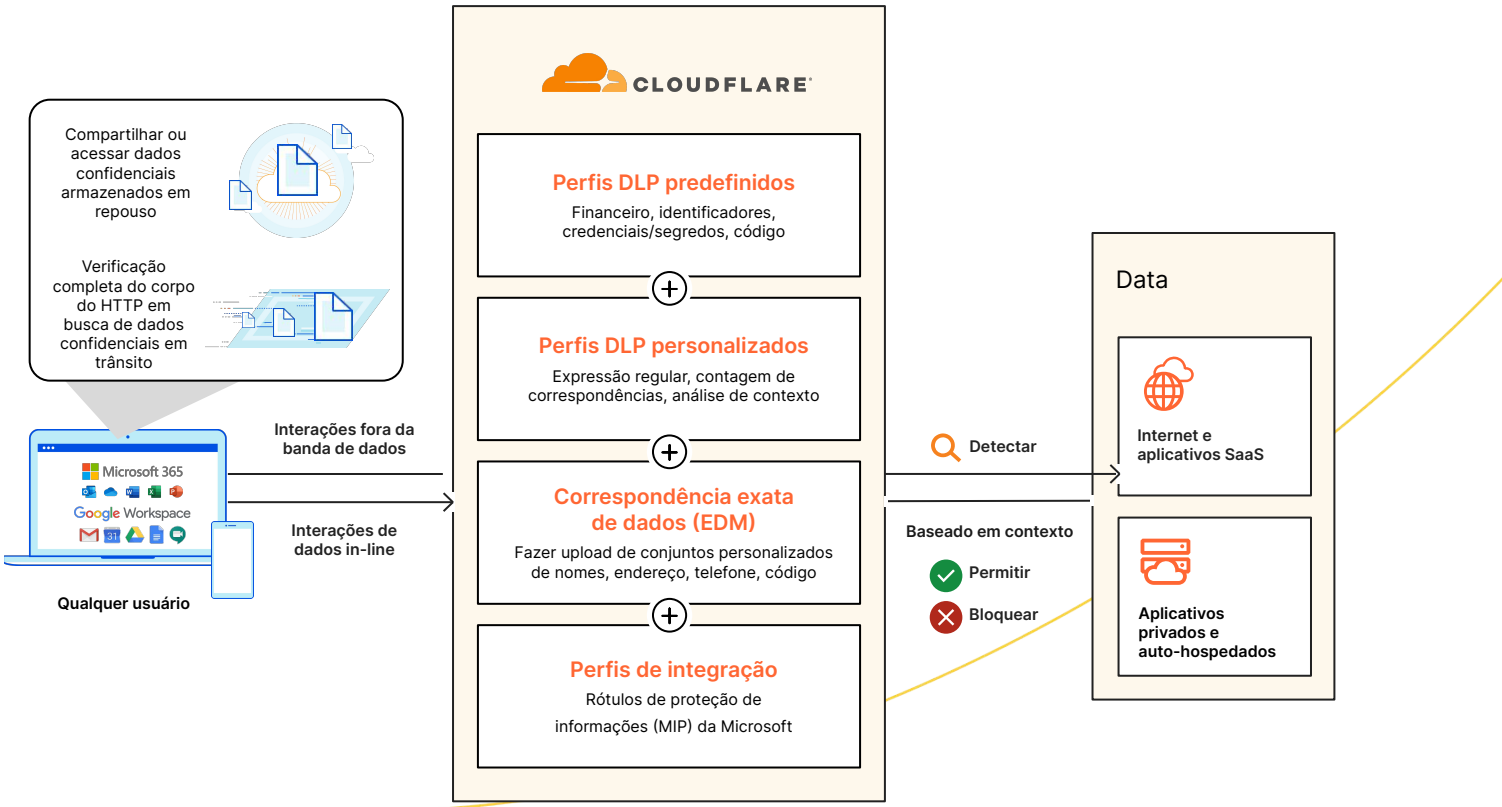
Os requisitos de conformidade estão ficando mais rígidos e abrangentes. Habilitar rapidamente perfis DLP predefinidos para analisar o tráfego de rede dos funcionários e bloquear o compartilhamento de dados regulamentados, como informações de identificação pessoal, PHI e outras informações financeiras (por exemplo, números de cartões bancários/de crédito).

Personalização avançada para necessidades de dados em constante mudança

A definição de dados confidenciais pode variar drasticamente entre organizações, dependendo do setor e dos locais de operação. Aplicar controles granulares a outros tipos de dados, como segredos, código, credenciais e IP, criando perfis DLP personalizados com análise de contexto e correspondência exata de dados.

Integração perfeita com ferramentas de classificação de dados existentes.

Manter um inventário completo de dados confidenciais é um grande avanço para as equipes de segurança e, portanto, requer ferramentas de classificação de dados como o MIP. Aumente a agilidade, e não a complexidade, com nossas integrações que recuperam automaticamente rótulos de confidencialidade e preenchem um perfil DLP.



Como o CASB funciona

O SSE construído nativamente oferece CASB in-line para controle de dados consistente em todos os aplicativos e dispositivos

Cada aplicativo SaaS requer considerações de segurança diferentes e opera fora das salvaguardas do perímetro tradicional. À medida que as organizações adotam dezenas de aplicativos SaaS, torna-se cada vez mais desafiador manter segurança, visibilidade e desempenho consistentes.

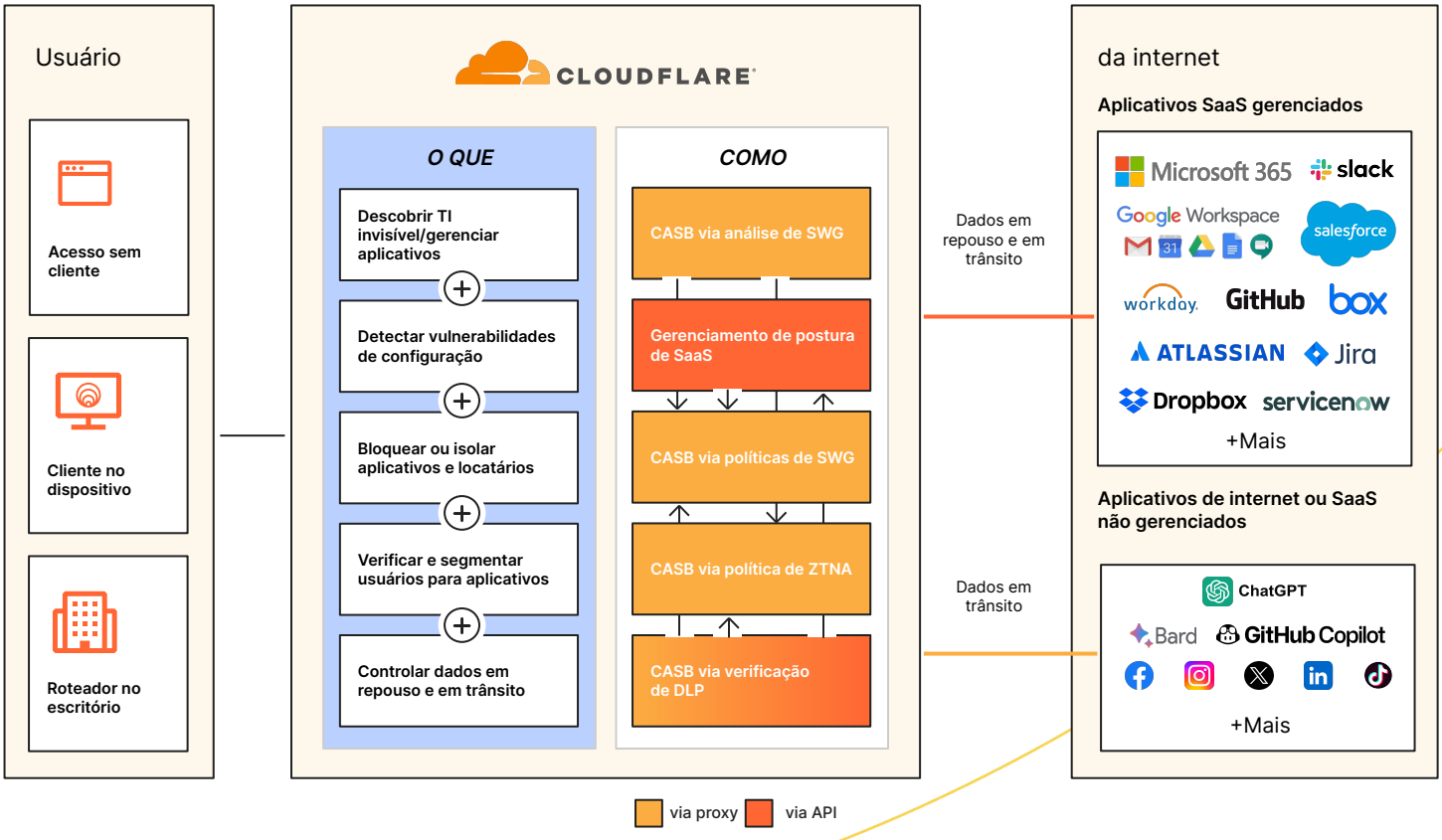
Para proteger os dados em trânsito, nosso CASB in-line coloca os controles ZTNA, SWG e isolamento do navegador remoto na frente de seus aplicativos.

- Registre todas as solicitações HTTP para revelar a TI invisível
- Bloquear/isolar compartilhamento de dados arriscado e com ameaças
- Acesso seguro a qualquer aplicativo SaaS

As integrações fáceis de API com CASB fornecem visibilidade rápida dos riscos em seus aplicativos SaaS gerenciados

Conecte-se a aplicativos SaaS populares (Google Workspace, Microsoft 365 etc.) em apenas alguns minutos com integrações rápidas de somente leitura de APIs.

Mantenha uma postura de segurança SaaS forte e capacite suas equipes de TI e segurança com visibilidade de permissões, configurações incorretas, acesso impróprio e problemas de controle que podem colocar seus dados e funcionários em risco. Em seguida, corrija rapidamente as ameaças identificadas pelo CASB com políticas SWG de fácil aplicação e verificação DLP integrada.



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, o que nos permite aproveitar as vantagens da IA com segurança...

De agora em diante, estamos entusiasmados com as inovações contínuas da Cloudflare para proteger dados e, em particular, com sua visão e roteiro para serviços como DLP e CASB."

- Applied Systems, Tanner Randolph, CISO

APPLIED

A Cloudflare substituiu as soluções pontuais Zscaler ZIA e Cisco AnyConnect VPN.

De forma mais ampla, ajudou a Applied Systems a consolidar a segurança entre funcionários, aplicativos e redes.

Leia o estudo de caso

O que os analistas dizem

FORRESTER

A Cloudflare foi nomeada como Strong Performer no The Forrester Wave™: Zero Trust Platforms, T3 de 2023.

A Cloudflare cita um momento contínuo de crescimento disruptivo no mercado de SSE, demonstrado por meio do reconhecimento de analistas, recebendo as pontuações mais altas possíveis, 5/5, nos critérios de inovação, roteiro, flexibilidade e transparência de preços e de capacitação e proteção da força de trabalho híbrida.

De acordo com o relatório, *"as diversas políticas de rede, DLP e controle de acesso da Cloudflare são gerenciadas a partir de um único console, permitindo que os clientes implantem e se protejam rapidamente contra ameaças originadas na internet."*

Leia o relatório completo

Gartner®

Cloudflare é o único novo fornecedor no Gartner® Magic Quadrant™ for SSE de 2023.

A Cloudflare foi reconhecida no relatório Gartner® Magic Quadrant™ for Security Service Edge (SSE) de 2023. Acreditamos que nosso reconhecimento valida nosso compromisso de continuar avançando em nossa plataforma Zero Trust para ajudar a proteger o trabalho híbrido.

Leia o relatório completo

Recursos de DLP integrados

Perfis de DLP	Definir os padrões de dados que você deseja detectar. • **Perfis DLP predefinidos:** informações financeiras (por exemplo, números de cartão de crédito), identificadores nacionais (informações de identificação pessoal), informações de saúde (PHI), credenciais e segredos (por exemplo, chaves GCP/AWS) e código-fonte • **Perfis personalizados**: criar detecções personalizadas para identificar tipos únicos de dados confidenciais (por exemplo, nomes de projetos internos, nomes de produtos não lançados)
Classificação de dados	Integrar o DLP com provedores de classificação de dados de terceiros, como rótulos de confidencialidade de proteção de informações da Microsoft (MIP). Recuperar informações de classificação do provedor, preencher o perfil DLP da Cloudflare e habilitar a política para permitir ou bloquear dados correspondentes.
Contagem de correspondências	Definir contagens de correspondências personalizadas para o número de vezes que qualquer entrada habilitada no perfil puder ser detectada antes que uma ação seja acionada, como bloqueio ou registro.
Análise de contexto	Análise de contexto para restringir as detecções de DLP com base em palavras-chave de proximidade (aproximadamente 1.000 bytes de distância).
Conjuntos de dados personalizados	Analisar o tráfego da web e de aplicativos SaaS para obter dados específicos definidos em um conjunto de dados personalizado. Para confidencialidade, pode editar/fazer hash de dados em logs. • **Correspondência exata de dados:** especificar os conjuntos de informações de identificação pessoal mais importantes, como nomes, endereços, números de telefone e números de cartão de crédito de clientes. Todos os dados são criptografados antes de chegar à Cloudflare. • **Listas de palavras personalizadas:** proteger dados não confidenciais, como propriedade intelectual e números de SKU.

Recursos do CASB multimodo

Visibilidade de risco e conformidade	
Verificação baseada em API	Integrar aplicativos SaaS de terceiros para verificar dados em repouso em busca de descobertas de segurança, como configurações incorretas, atividades de usuários não autorizadas, TI invisível e problemas de segurança de dados que podem ocorrer após o login bem-sucedido de um usuário. Mais de 18 integrações disponíveis (por exemplo, Microsoft 365, Google Workspace).
Detecção da TI Invisível	Visibilidade de TI invisível nos aplicativos SaaS e nas origens da rede privada que seus usuários finais estão visitando. Analisar os aplicativos descobertos e ajustar o status de aprovação: Aprovado, Reprovado, Em análise e Não analisado. Definir políticas granulares de identidade e baseadas em dispositivos* adequadamente.
Registros de auditoria	Registro abrangente* para todas as solicitações, usuários e dispositivos. Usar logpush* ou API para integração com armazenamento de terceiros existente ou ferramentas SIEM para auditoria de conformidade.
Segurança de dados e prevenção de ameaças	
Acesso Zero Trust*	Definir políticas de menor privilégio por aplicativo via ZTNA para limitar o acesso de usuários aos dados
Controles de compartilhamento de arquivos*	Permitir ou bloquear uploads/downloads de arquivos com base no tipo MIME por meio de políticas HTTP SWG
Controles de aplicativos*	Permitir ou bloquear o tráfego para aplicativos específicos ou tipos de aplicativos por meio de políticas HTTP SWG
Controles do locatário*	Controlar o tráfego de locatários de aplicativos SaaS por meio de SWG para evitar a perda de dados
Controles do navegador*	Proteger os dados em uso em um navegador restringindo ações de download, upload, copiar/colar, entradas por teclado e ações de impressão isoladas nas páginas web e nos aplicativos através do isolamento do navegador remoto. Evitar o vazamento de dados em dispositivos locais e controlar as inserções de usuários em sites suspeitos.
Verificação de DLP*	Examinar o tráfego HTTP via SWG em busca de dados confidenciais por meio de strings que correspondam às palavras-chave ou RegEx especificados em configurar perfil DLP. Habilitar perfis DLP em uma integração CASB e descobrir se os arquivos armazenados em seus aplicativos SaaS contêm dados confidenciais. Estender o DLP para aplicativos privados por meio de isolamento do navegador remoto sem cliente, que herda todas as políticas baseadas em HTTP.

**usando recursos de ZTNA, SWG e isolamento do navegador remoto na plataforma SSE e SASE*

Por que a Cloudflare?

Uma plataforma unificada

Acesso seguro verificando e segmentando qualquer usuário para qualquer recurso

Defesa contra ameaças cobrindo todos os canais com IA/ML alimentados por rede e inteligência contra ameaças

Proteção de dados aumentando a visibilidade e o controle dos dados em trânsito, em repouso e em uso

Uma rede programável

Mais eficaz ao simplificar a conectividade e gerenciamento de políticas

Mais produtivo ao garantir UX rápida, confiável e consistente em todos os lugares

Mais ágil ao inovar rapidamente para atender aos seus requisitos de segurança em constante evolução

Pronto para discutir suas necessidades de proteção de dados?

Solicitar workshop

Ainda não está pronto para uma conversa ao vivo?

Continue aprendendo mais sobre a plataforma SSE e SASE da Cloudflare

1. 2023 survey: techvalidate.com/product-research/cloudflare/charts
2. IBM Cost of Breach Report: https://www.ibm.com/reports/data-breach