Prevenção contra perda de dados

Proteja dados sensíveis e garanta a conformidade regulatória em aplicativos web, privados, SaaS, em nuvem, de IA e e-mail.

A prevenção contra perda de dados (DLP) mais integrada para a era agêntica

Com o Cloudflare DLP, você pode detectar e bloquear a exfiltração de dados sensíveis em toda a sua rede e aplicativos (SaaS, de IA, em nuvem, privados e e-mail) sem interromper ou diminuir a produtividade dos usuários.

Proteja sua propriedade intelectual, código-fonte, informações de identificação pessoal de clientes e outros dados para:

- **Impor conformidade** usando perfis pré-criados para dados financeiros, registros médicos e números de seguridade social.
- **Proteger dados corporativos** bloqueando uploads confidenciais para armazenamento em nuvem ou sites de compartilhamento de arquivos não autorizados.
- **Proteger prompts de IA** verificando e editando dados sensíveis ou código-fonte em entradas de ferramentas como ChatGPT e GitHub.
- **Obter visibilidade sobre a movimentação de dados** em toda a sua força de trabalho híbrida.

Desenvolvido na borda global da Cloudflare, a inspeção ocorre a milissegundos do usuário, garantindo uma proteção rápida e econômica em escala.

Provedor de infraestrutura

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

Leia o estudo de caso

Banco digital líder

Consolidou a segurança em um único painel, garantindo a conformidade rigorosa de dados e a proteção contra ransomware para sua plataforma bancária que prioriza dispositivos móveis.

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

Segurança de SaaS e IA simplificada

Controle o uso da IA pela força de trabalho bloqueando conteúdo suspeito e reduza os riscos de exfiltração identificando e corrigindo dados sensíveis armazenados em ambientes SaaS e em nuvem.

Gerenciamento unificado de políticas

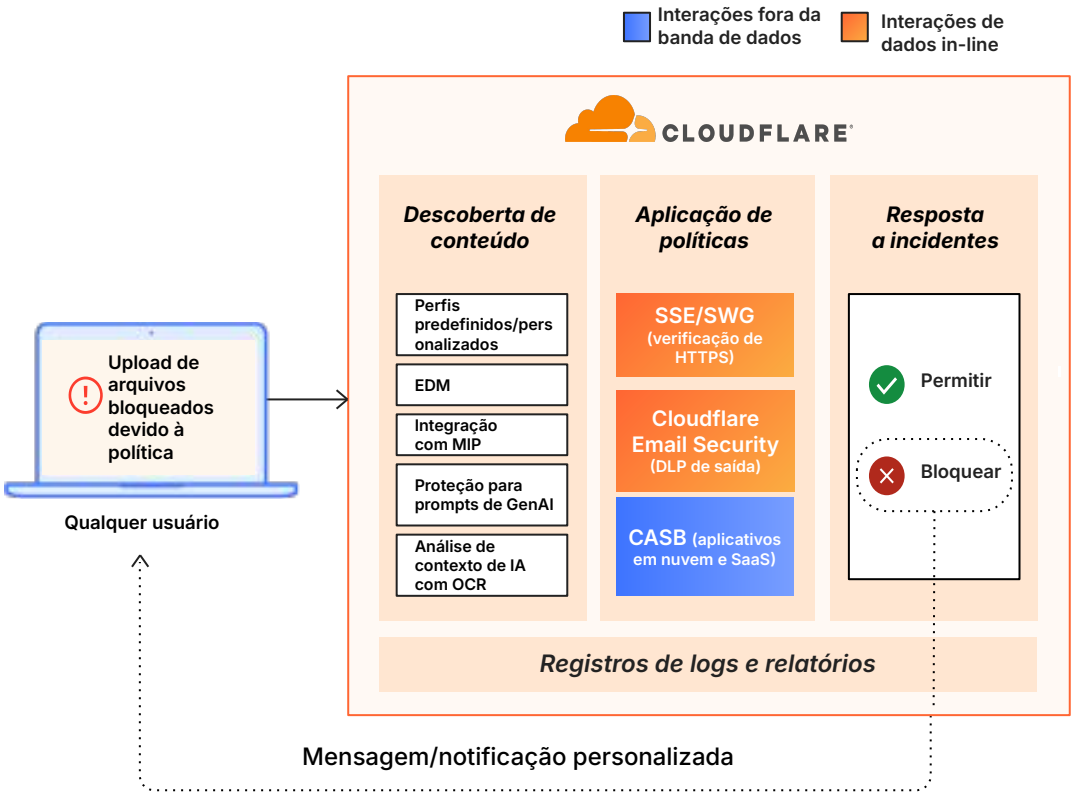
Configure perfis de DLP, entradas de detecção e rótulos de confidencialidade do Microsoft Purview para consolidar as proteções no tráfego de saída, documentos, PDFs e imagens.

Controles de dados adaptativos

Forneça feedback por detecção para treinar a análise de contexto de IA e melhorar a precisão da detecção. O DLP se adapta aos seus padrões de dados e tráfego específicos para reduzir falsos positivos.

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

Proteção de dados em todos os canais do espaço de trabalho



Como funciona

O Cloudflare DLP oferece inspeção automatizada e com reconhecimento de contexto em tráfego HTTPS e de e-mail.

Criado nativamente na estrutura Zero Trust da Cloudflare, ele elimina lacunas de segurança ao consolidar a proteção de dados em uma plataforma única e unificada, garantindo visibilidade e controle contínuos em todos os canais.

Exemplos de recursos do DLP	
Perfis do DLP	Implantar perfis predefinidos para informações de identificação pessoal, PHI, dados financeiros e credenciais, ou criar perfis personalizados para proteger ativos proprietários, como nomes de projetos internos ou propriedade intelectual não divulgada.
Proteção de Informações da Microsoft (MIP)	Importar rótulos de confidencialidade MIP para aplicar políticas automaticamente (por exemplo, bloquear "Confidencial") sem reclassificar arquivos.
Correspondência exata dos dados (EDM)	Fazer upload de conjuntos de dados hash (por exemplo, um banco de dados de clientes específico) para detectar valores exatos em vez de padrões genéricos. Bloquear registros específicos e reduzir drasticamente os falsos positivos.
Impressão digital de documentos	Proteger documentos confidenciais criando e armazenando "impressões digitais" exclusivas (hashes/padrões) que são comparadas com o tráfego de rede para identificar e bloquear documentos semelhantes.
Proteção para prompts de GenAI	Evitar que dados sensíveis (código-fonte, informações de identificação pessoal de clientes) sejam colados em LLMs públicos. Inspecionar solicitações HTTPS para ferramentas como ChatGPT ou Gemini para impor o uso seguro de IA.
Análise de contexto de IA e pontuação de confiança	Usar aprendizado de máquina para analisar palavras-chave de contexto e proximidade. Definir limites de confiança para bloquear automaticamente correspondências de alto risco e registrar logs de eventos de menor confiança para ajuste.
Reconhecimento óptico de caracteres (OCR)	Digitalizar e extrair texto automaticamente de arquivos de imagem (PNG, JPG/JPEG) para evitar que os usuários contornem a segurança fazendo capturas de tela de documentos confidenciais.
Treinamento e instrução de usuários	Exibir notificações personalizáveis em tempo real que instruem instantaneamente os usuários sobre violações das políticas de segurança.
Análise forense e registros de logs unificados	Combinar o registro de logs de eventos granular com a inspeção segura de conteúdo malicioso. Analisar trechos de dados específicos e o contexto do usuário para validar incidentes instantaneamente e ajustar políticas.

