

Cloudflare API Shield

Gerenciar e proteger as APIs que impulsionam as empresas

Desafios das APIs modernas

Na mira dos invasores

As APIs movem o mundo. Cinquenta e oito por cento do tráfego HTTP dinâmico na rede da Cloudflare está relacionado a APIs.

As APIs apresentam empolgantes oportunidades de negócios para entregar produtos mais rapidamente e aprimorar a experiência do cliente. Hoje, os líderes de segurança precisam equilibrar a segurança de suas APIs e de seus aplicativos web, sem desacelerar a inovação.

As equipes de segurança e TI precisam proteger os dados confidenciais de seus clientes e, ao mesmo tempo, permitir as operações da empresa em aplicativos web e propriedades de APIs.

Afinal, é a confiança do cliente que está em jogo.



Cloudflare API Shield

Os clientes podem descobrir, proteger e simplificar a segurança e o gerenciamento de suas APIs públicas consolidando seus aplicativos web e a proteção de APIs na borda da Cloudflare.

O API Shield faz parte do portfólio de segurança de aplicativos da Cloudflare, que também detém bots, impede ataques de DDoS, bloqueia ataques a aplicativos e monitora ataques à cadeia de suprimentos.



Riscos das APIs ocultas

As equipes de desenvolvimento geralmente publicam novas APIs sem informar a TI, portanto, as APIs operam nas sombras, sem gerenciamento ou segurança.



Preocupações com autenticação, perda de dados e violação

Depois que as APIs são descobertas, elas devem ser protegidas contra ataques e violações com autenticação, validação de esquema, proteções contra violação de APIs e detecções de exfiltração de dados.



Monitoramento do desempenho de APIs

Considerando que as APIs impulsionam as empresas, uma vez que estejam monitoradas e protegidas, as empresas precisam acompanhar seu desempenho: entender volumes de requisições por endpoint, taxas de erro e latência.

Cloudflare API Shield

Gerenciar e proteger as APIs que impulsionam as empresas

Principais recursos

Descoberta e gerenciamento de APIs

Descoberta e aprendizado de esquema	Descobrir endpoints de API em uso ativo e seus esquemas associados por meio de modelos orientados por aprendizado de máquina e baseados em heurísticas.
Análise de sequência e desempenho	Descobrir as sequências mais importantes do comportamento de chamadas de API e analisar o desempenho de endpoints de API (por exemplo, solicitações, latência, taxa de erro, tamanho da resposta etc.).
Portal para desenvolvedores e gerenciamento	Gerenciar a documentação de APIs interativas e hospedar em seu domínio com o Cloudflare Pages.

Postura de segurança para APIs

Detecção de ataques de BOLA	
Postura de autenticação	Verificações de risco que identificam e alertam sobre configurações incorretas de autenticação em APIs, como nenhuma autenticação ou autenticação combinada (onde apenas em algumas chamadas de API para um endpoint solicitam direitos de acesso).
Detecção de dados confidenciais	Detectar dados confidenciais nas respostas de APIs que saem de sua origem e emitir alerta por endpoint.

Proteção do tempo de execução de APIs

Validação de autenticação	Autenticar e validar o tráfego de APIs com certificados mTLS, tokens web JSON (JWT), chaves de API e tokens OAuth 2.0 para bloquear solicitações de clientes ilegítimos.
Validação de esquema	Usar esquemas de API para aceitar chamadas de API válidas e bloquear solicitações malformadas e anomalias de HTTP. Isso complementa o modelo de segurança negativo do Cloudflare WAF para segurança abrangente.
Proteção contra violação de REST e GraphQL	Interromper a violação volumétrica e sequencial com sugestões de limitação de taxa baseadas em sessão por endpoint. Estender as proteções contra negação de serviço (DoS) aos endpoints de GraphQL.

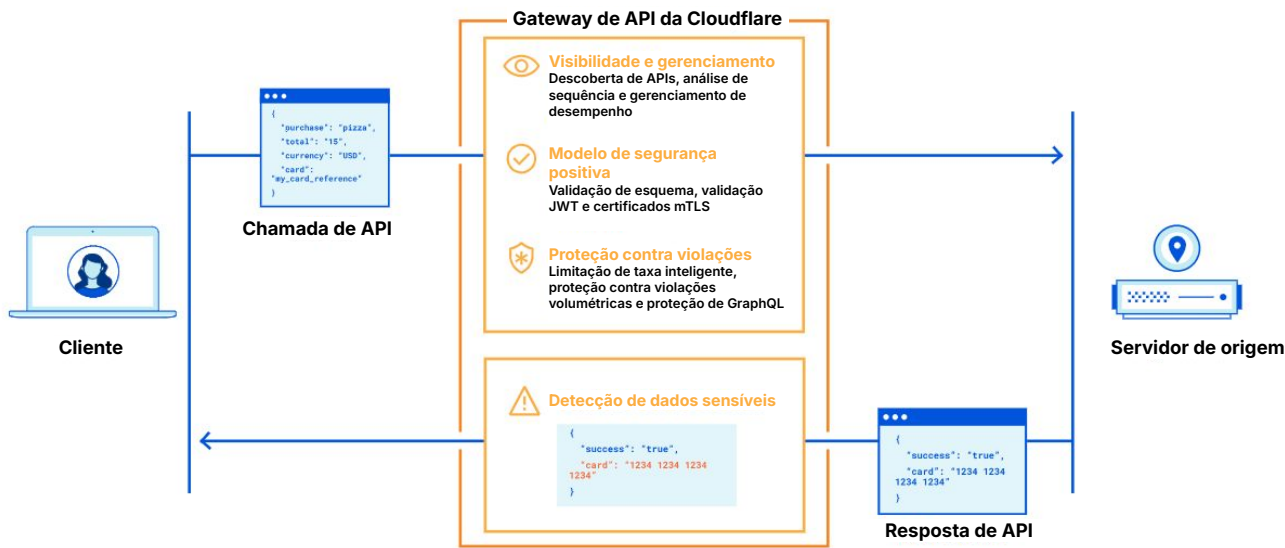


Figura 1: Arquitetura do Cloudflare API Shield

Liderança da Cloudflare

O portfólio de segurança de aplicativos da Cloudflare recebeu vários elogios por sua força e amplitude. A Cloudflare foi nomeada Líder no mais recente Forrester Wave: Web Application Firewalls. A Gartner nomeou a Cloudflare como líder de escolha dos clientes em soluções de mitigação de DDoS em 2023 no Gartner® Peer Insights™ “Voice of the Customer”: DDoS Mitigation Solutions. A Forrester indicou a Cloudflare como Strong Performer no The Forrester Wave™: Bot Management Software, T3 de 2024. O IDC indicou a Cloudflare como um player importante no IDC MarketScape for Web Application and API Protection (WAAP) Enterprise Platforms de 2024.