CLOUDFLARE

FICHA TÉCNICA

API Shield Cloudflare

Com a Cloudflare como seu gateway de segurança de APIs, as APIs vão impulsionar os negócios como nunca.

As APIs movem o mundo. Cerca de 58% do tráfego global da internet está relacionado a APIs. Os invasores sabem disso. A Gartner estima que as APIs logo se tornarão o vetor de ataque mais frequente.

O Cloudflare API Shield mantém as APIs seguras e produtivas com descoberta de APIs e defesas inovadoras em camadas. O API Shield faz parte do portfólio de segurança de aplicativos da Cloudflare, que também detém bots, impede ataques DDoS, bloqueia ataques de aplicativos e monitora ataques à cadeia de suprimentos.

Nossos produtos de segurança de aplicativos funcionam em estreita cooperação com nosso pacote de desempenho e são fornecidos pela plataforma global em nuvem mais conectada do mundo.

Inovação de segurança de APIs

O API Shield descobre todas as APIs em uso e fornece segurança de APIs em camadas ao mesmo tempo. Nossas proteções contra DDoS de primeira categoria nas camadas de rede e de aplicação acompanham o API Shield para mais proteção.

Descoberta de APIs

A descoberta automática de APIs elimina as APIs ocultas, garantindo que todos os endpoints de API sejam descobertos e monitorados para um melhor gerenciamento de APIs.

Autenticação mais forte

Verifica a identidade baseada em certificado com TLS mútuo (mTLS). Esse modelo de lista de permissões, gerenciado pela Cloudflare, é importante para dispositivos móveis e de IoT, bloqueando solicitações sem um certificado válido. A Cloudflare também verifica as credenciais roubadas que estão sendo usadas.

Validação de esquema de APIs

APIs seguras com um modelo de segurança positivo, que se aplica a um esquema de APIs. Com um esquema OpenAPI v3 instalado, as solicitações são validadas automaticamente em relação a ele. Quaisquer operações que não estejam em conformidade com o esquema são bloqueadas.

Parar o abuso e a perda de dados

A detecção avançada de anomalias detém o tráfego abusivo e volumétrico de APIs com base na compreensão do volume específico de uma API. A rede da Cloudflare também oferece prevenção contra perda de dados que detecta e bloqueia a exfiltração de informações confidenciais em respostas de APIs.

Principais riscos à segurança de APIs

Dados os desafios de segurança que as APIs apresentam, o OWASP divulgou uma lista dos dez principais riscos à segurança de APIs que devem ser considerados. A Cloudflare ajuda com todos os riscos de APIs do OWASP - veja algumas das principais preocupações descritas abaixo.

Falha de autorização em nível de objeto

A falha de autorização em nível de objeto (BOLA) é a manipulação de IDs de objetos em uma solicitação para obter acesso não autorizado a dados confidenciais. Com a BOLA, os invasores acessam objetos (dados) aos quais não deveriam ter acesso, apenas alterando os IDs.

Falha de autenticação de usuário

A autenticação é essencial, mas muitas vezes é implementada de forma inadequada. Os invasores exploram falhas (ou falta de autenticação) para fazer login de forma ilícita ou assumir a identidade de outro usuário. A segurança de APIs fica comprometida se os sistemas não conseguirem autenticar clientes/usuários corretamente.

Falta de recursos e Rate Limiting

Sem proteções adequadas contra abuso e limites de taxa que restrinjam o tamanho ou o número de recursos solicitados, as APIs ficam suscetíveis a ataques de força bruta e negação de serviço, enquanto o desempenho do servidor de APIs é prejudicado.

Gestão de ativos inadequada

O gerenciamento inadequado de ativos ocorre quando não há nenhuma descoberta de APIs que rastreie as APIs de produção atuais e aquelas que ficaram obsoletas, levando a APIs ocultas ou não autorizadas. Isso também pode ocorrer por meio de um registro de atividade de APIs insatisfatório.

Segurança de aplicativos de excelência

Proteção mais precisa

Buscamos sempre um equilíbrio entre a segurança e os negócios com proteções precisas contra ameaças a APIs, bots e ataques A Cloudflare foi testada e ajustada pelas maiores empresas.

Vasta capacidade integrada

Não unimos bases de código de aquisição de forma negligente. Em vez disso, a segurança integrada, a partir de um único console, aprimora constantemente sua capacidade de parar ameaças. O desempenho na forma de CDN, DNS e aceleração de tráfego está integrado.

Posturas de segurança abrangentes

Oferecemos recursos de segurança completos, prontos para a empresa e econômicos. Nunca vamos explorá-lo com ofertas básicas limitadas que exigem complementos caros ou integrações de mercado de terceiros para uma forte postura de segurança.

Liderança da Cloudflare

As organizações obtêm uma postura de segurança de aplicativos mais eficaz com a rede global da Cloudflare como perímetro de segurança empresarial. O portfólio de segurança de aplicativos da Cloudflare recebeu vários elogios por sua força e amplitude. A Gartner nomeou o Cloudflare WAF como Preferência do Cliente em 2021. A Frost & Sullivan reconheceu a Cloudflare como líder em inovação em proteção da web integral e global, enquanto a IDC e a Forrester escolheram a empresa como líder em DDoS.

© 2022 Cloudflare Inc. Todos os direitos reservados. O logotipo da Cloudflare é uma marca registrada da Cloudflare. Todos os demais nomes de produtos e de outras empresas podem ser marcas registradas das respectivas empresas às quais estamos associados.

+55 (11) 3230.4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:BDES/3948.2022NOV4