CLOUDFLARE

RESUMO DO PRODUTO

Bot Management da Cloudflare

Bloqueie bots maliciosos e gerencie bots de IA sem a necessidade de CAPTCHAs.

Os bots se ocultam em seu tráfego. Bots maliciosos prejudicam a receita e a UX.

Trinta porcento do tráfego de aplicativos na internet é tráfego automatizado[1]. Defesas tradicionais, como heurísticas baseadas em geografia e IP, assim como os desafios CAPTCHA, são facilmente contornadas por bots modernos. Isso frustra muito os usuários reais.

Com visibilidade de **cerca de 20%** da web, ninguém identifica mais crawlers de IA e bots de pesquisa do que a Cloudflare[2].

O **Bot Management da Cloudflare** ajuda as organizações a gerenciar crawlers de IA e tráfego de bots para aplicativos web e móveis sem CAPTCHAs. Permite que bots verificados e crawlers de IA compatíveis acessem aplicativos, ao mesmo tempo em que desafia e impede bots de IA não compatíveis e bots maliciosos. Este é um recurso fundamental em nosso portfólio de segurança de aplicativos.

Benefícios do produto

- Proteger contra fraudes, perdas financeiras e danos à reputação da marca
- Oferecer experiências melhores para aplicativos web e em dispositivos móveis
- Conquistar a independência de crawlers de IA e bots de pesquisa indesejados

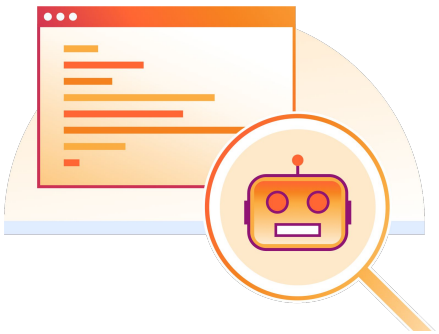

Figura 1: Bot Management da Cloudflare integrado em nosso portfólio de segurança de aplicativos

Fontes

1. Dados do Cloudflare Radar, 2024
2. W3techs, Usage statistics and market shares of reverse proxy services, 2025

Como o Bot Management da Cloudflare funciona

A Cloudflare combina detecção multicamadas de aprendizado de máquina global e específico do aplicativo, JavaScript do lado do cliente, dispositivos móveis e heurísticas em uma única pontuação de bots fornecida a cada solicitação HTTP. Uma pontuação de bots indica a probabilidade de que essa solicitação tenha vindo de um bot. Essa pontuação de bots é usada para respostas padrão, como bloquear ou permitir, e para políticas de respostas personalizadas por meio de outros produtos da Cloudflare. As análises de bots, incluindo a pontuação de bots, os metadados de solicitações HTTP e outros dados, estão disponíveis na interface do usuário do painel da Cloudflare ou por meio da API da Cloudflare em ferramentas de terceiros.

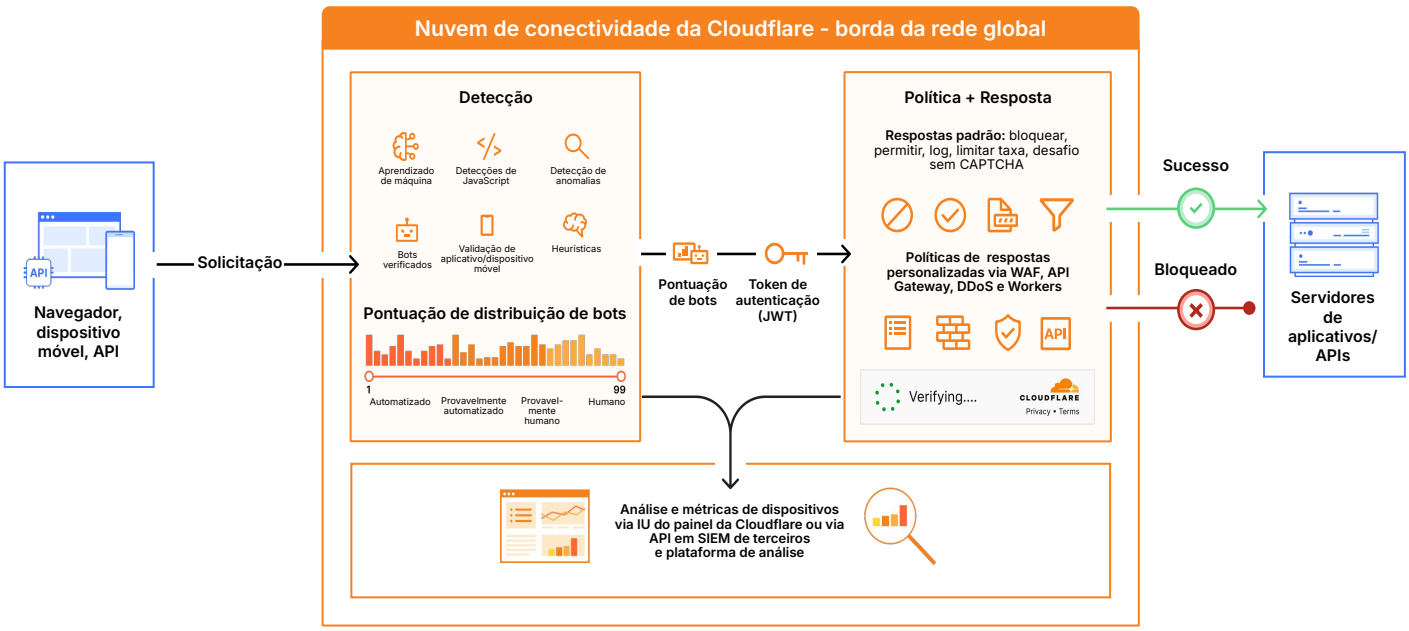

Figura 2: Exemplo de caminho de solicitação através do Bot Management da Cloudflare

Principais recursos do Bot Management da Cloudflare

Violação e controle de conta

Proteja-se contra ataques de dia zero com modelos apoiados por ML que podem detectar vulnerabilidades mais rápido do que a divulgação pública. Defenda-se contra ataques de DDoS recordes, proteja dados confidenciais, reduza riscos do lado do cliente e monitore a cadeia de suprimentos de software de seus aplicativos web.

Defender contra bots e fraudes

Proteja seus usuários contra controle de conta e detenha bots ruins que afetam a experiência do usuário final. Pare botnets maliciosas, preenchimento de credenciais e cartões, raspagem de conteúdo e acumulação de estoque, combinando modelos de ML com inteligência contra ameaças, de clientes e de rede.

Gerenciar crawlers e bots de IA

Exerça maior controle sobre conteúdo e custos bloqueando crawlers de IA, cobrando-os ou prendendo-os em loops intermináveis. Tenha visibilidade dos padrões de solicitação e da conformidade com as suas diretivas robots.txt. Disponível para todos os clientes da Cloudflare.

Principais recursos	
Mecanismos de detecção	
Aprendizado de máquina	Nosso modelo global de aprendizado de máquina é treinado em todo o tráfego da rede global da Cloudflare, que serve como proxy para bilhões de solicitações diariamente, para identificar tráfego automatizado e humano. Ele está incluído em nossa pontuação de bots geral. Os clientes são atualizados automaticamente para o modelo mais recente.
Detecção de anomalias	Nossos modelos de anomalia comportamental de aprendizado não supervisionado estabelecem padrões de tráfego específicos de aplicativos e calibram os limites das regras para identificar o comportamento anômalo de bots à medida que os padrões de tráfego dos clientes mudam ao longo do tempo. Isto está incluído em nossa pontuação de bots geral.
Heurísticas	Utilizamos padrões conhecidos de comportamento de bots ruins provenientes de tráfego de bots anterior para identificar bots. Atualizamos regularmente nossas heurísticas para todos os clientes. Isto está incluído em nossa pontuação de bots geral.
Bots verificados e bots de IA	Nosso diretório de bots identifica IDs de detecção de bots conhecidos que desempenham funções legítimas e operam de forma transparente como bots verificados, conforme prescrito pela política de bots verificados da Cloudflare. Temos uma categoria separada para bots de IA conhecidos, que podem ou não respeitar o robots.txt e ocultar seu comportamento de seus aplicativos.
Detecção de JavaScript	O módulo de detecção JavaScript identifica navegadores sem cabeçalho e outras impressões digitais maliciosas por meio de uma injeção JavaScript leve e invisível no lado do cliente de qualquer solicitação. Honramos padrões de privacidade muito rígidos e não coletamos informações de identificação pessoal durante o processo.
Pontuação de bots	Usar a pontuação de bots para escrever menos regras para capturar a maioria dos bots, em vez de escrever uma regra para cada ID ou tipo de bot. A pontuação de bots combina a inteligência de nossos mecanismos de detecção para produzir uma pontuação de 1 a 99 que indica a probabilidade de uma solicitação ter sido originada por um bot. Uma pontuação 1 refere-se a solicitações definitivamente automatizadas, e 99 refere-se a solicitações definitivamente humanas.
Validação de dispositivo via SDKs de dispositivo móvel	Esses SDKs para todas as principais plataformas de aplicativos móveis, incluindo Android, iOS, React Native, Unity e outras, validam a integridade do aplicativo, detectam ambientes inseguros e autenticam o tráfego de APIs (com tokens criptográficos fornecidos por você ou aprovados pela Cloudflare).
Política e resposta	
Respostas padrão	Configurar bloquear, permitir, log, limite de taxa ou uma variedade de desafios fáceis de usar como respostas ao tráfego de bots identificado por nossos mecanismos de detecção.
Políticas de respostas personalizadas	Incorporar os sinais do Bot Management nas políticas de outros produtos da Cloudflare, como Cloudflare WAF e DDoS, e criar ações personalizadas por meio do Workers.
Análises	
Painel da Cloudflare	Analisar a atividade de bots dos últimos trinta dias e filtrar por pontuação de bots e outros filtros de bots, tráfego e solicitações. O ciclo de feedback de bots permite que os clientes informem à Cloudflare quaisquer falsos positivos ou falsos negativos para investigação posterior.
Ferramentas de terceiros (SIEM, data lake, ferramentas de análise, etc.)	Analisar os sinais do Bot Management em todos os seus aplicativos em um único painel por meio da análise de segurança da Cloudflare, explorar dados de registro adicionais no Log Explorer e combinar dados de terceiros com os da Cloudflare em um SIEM ou plataforma de análise de terceiros por meio do Log Push.

Tem interesse em ver mais? Inscreva-se em nossa série de demonstrações de segurança de aplicativos.