CLOUDFLARE

RESUMO DA SOLUÇÃO

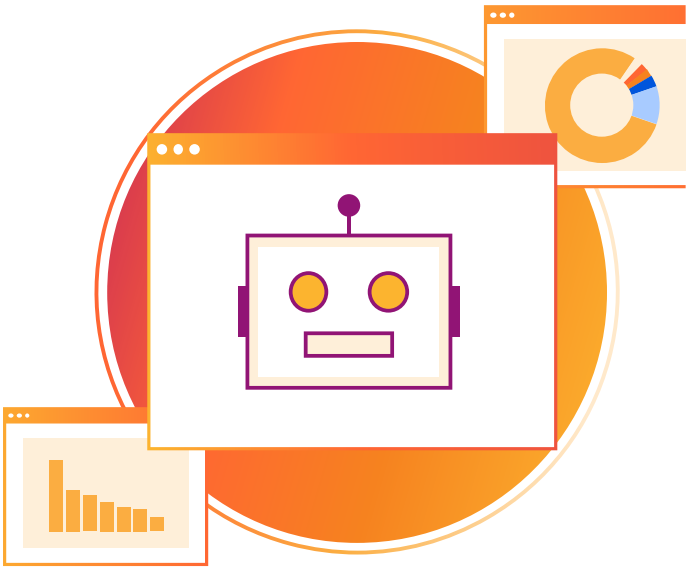
# Quatro estratégias para gerenciamento de bots maliciosos

Evite danos dispendiosos e perda de receita por causa de bots indesejados

## Os bots estão por toda parte na internet

Os bots são comuns na internet moderna porque ajudam a automatizar tarefas importantes. Estima-se que de 40 a 50% do tráfego total da internet seja gerado por bots e muitos desses bots desempenham funções comerciais legítimas.

No entanto, os bots também são frequentemente usados por criminosos para atacar ativos da web e causar danos dispendiosos. Bots maliciosos podem roubar dados, invadir contas de usuários, enviar dados indesejados por meio de formulários on-line e realizar outras atividades maliciosas. Eles desperdiçam recursos preciosos de computação e de sites, roubam dados e distorcem a análise do tráfego.



### O que é gerenciamento de bots?

O gerenciamento de bots se destina a bloquear o tráfego de bots indesejados ou maliciosos e, ao mesmo tempo, permitir que os bots úteis acessem os ativos da web. Para atingir esses objetivos, o gerenciamento de bots detecta a atividade de bots, diferencia os comportamentos desejáveis dos indesejáveis e identifica as origens das atividades indesejáveis.

### Por que isso é importante?

O gerenciamento de bots é necessário porque, se não forem verificados, os bots podem causar problemas enormes e dispendiosos. As organizações precisam garantir que não bloqueiam bots necessários, como bots de rastreamento de mecanismos de pesquisa, enquanto tentam filtrar qualquer tráfego de bots maliciosos para seus ativos da web.

### O que pode ser feito?

Identificar e bloquear bots maliciosos antes que eles lancem ataques é um componente essencial de qualquer boa estratégia de segurança. Compartilhamos quatro histórias de clientes reais da Cloudflare que enfrentaram seus desafios de gerenciamento de bots com quatro estratégias diferentes usando produtos da Cloudflare.

## Bloquear os bots

Essa abordagem requer cuidado porque muitos processos de negócios legítimos, como a indexação dos mecanismos de pesquisa, exigem que os bots possam acessar os recursos da empresa.

| Bloquear os bots | | |
|---|---|---|
| **Desafio** | **Solução** | **Resultados** |
| Uma empresa de iGaming notou um aumento significativo nas reclamações dos usuários. Suas contas estavam sendo hackeadas e as informações de cartão de crédito roubadas. Agentes maliciosos estavam usando bots automatizados para ataques de tentativas de quebra de senha com força bruta em credenciais de login, obtendo acesso a contas de usuários e, finalmente, controlando tais contas. | A equipe de segurança aplicou **limitação de taxa**, juntamente com o **Bot Management** avançado, para detectar várias tentativas de login em um curto espaço de tempo. Quando um comportamento incomum foi detectado, a limitação de taxa começou a bloquear automaticamente solicitações maliciosas. Desde a implementação do recurso de limitação de taxa, a empresa de iGaming não sofreu um único ataque de preenchimento de credenciais. | Todas as empresas precisam equilibrar segurança rigorosa com uma experiência de usuário ideal.<br><br>O conjunto de ferramentas certo pode ajudar a detectar e evitar o tráfego de bots maliciosos, minimizando falsos positivos e obstáculos para usuários reais. |

## Desacelerar o inimigo

Essa técnica maximiza o tempo de resposta para todas as solicitações de rede suspeitas.

| Desacelerar o inimigo | | |
|---|---|---|
| **Desafio** | **Solução** | **Resultados** |
| Uma empresa de apostas esportivas notou uma redução significativa nas transações.<br><br>Ao analisar o problema, eles identificaram uma atividade maliciosa de bots que estava extraindo as probabilidades do site e usando essas informações para obter uma vantagem competitiva. | A empresa não bloqueou os bots porque os agentes maliciosos contornaram o bloqueio. Em vez disso, ela reduziu a velocidade de coleta de dados para apostas.<br><br>Ela usou o **Headers Override** para marcar solicitações suspeitas com base na análise do **Bot Management**, seguida por scripts do **Workers** para reagir a esses cabeçalhos e desacelerar as solicitações. | Esse método permitiu à empresa restaurar a atividade normal dos usuários. Outros métodos incluem o uso de CAPTCHAs para solicitações de alto volume ou modificação da marcação HTML em intervalos regulares.<br><br>Essas ações interrompem o fluxo de trabalho dos bots para que a raspagem de conteúdo consistente se torne mais complicada. |

## Enganar os bots

Embora muitas empresas implementem contramedidas contra bots, um invasor realmente determinado pode contorná-las. Em vez disso, algumas empresas decidem revidar.

| Enganar os bots | | |
|---|---|---|
| **Desafio** | **Solução** | **Resultados** |
| Uma empresa de apostas esportivas tentou encontrar uma solução para bots que raspavam as probabilidades em seu site.<br><br>Após pensarem um pouco, decidiram lançar uma solução alternativa com vários produtos da Cloudflare que permitiam alimentar os bots com informações aleatórias. | Quando o sistema notava que uma solicitação tinha sido gerada por um bot malicioso, ele aceitava essa solicitação e gerava um novo fluxo de trabalho:<br><br>Solicitação → **WAF** (bot identificado) → **Bot Management** (atribuição de pontuação de ameaça) → **Workers** (geração de dados aleatórios) → **Workers** (retorno de dados aleatórios para o bot) | O novo fluxo de trabalho gerava novos dados aleatórios que eram devolvidos aos bots maliciosos.<br><br>Como resultado, os bots que vinham para coletar probabilidades e infligir danos iam embora com algo inútil, o que desencorajava qualquer violação adicional. |

## Realizar análise dinâmica

À medida que os bots se tornam mais sofisticados, as empresas precisam coletar dados sobre os bots e realizar análises dinâmicas antes de agir. Tais objetivos podem incluir a detecção de registros, probabilidades, reivindicações de bônus, etc. que são prejudiciais. Para garantir uma análise completa, as equipes de segurança podem precisar combinar várias fontes de dados de ferramentas internas e externas para analisar os parâmetros do tráfego de bots.

| Realizar análise dinâmica | | |
|---|---|---|
| **Desafio** | **Solução** | **Resultados** |
| Uma empresa de apostas lançou uma campanha de marketing para atrair novos usuários com recompensas pelo registro. Logo após o lançamento, eles notaram que os bots estavam fazendo registros falsos.<br><br>A empresa já tinha algumas ferramentas internas de análise, mas elas não ofereciam uma imagem completa do comportamento dos bots. | A equipe implementou o **Bot Management** avançado da Cloudflare com assinaturas JA3 para gerar **logs brutos** de todo o tráfego da internet que chegava à página de registro. Eles enriqueceram seus sistemas internos com pontuações de bots e assinaturas JA3, o que lhes permitiu identificar bots de forma mais clara. | Após análise minuciosa, a empresa conseguiu cancelar os registros falsos e evitar inflar as estatísticas de usuários recém-adquiridos.<br><br>Eles introduziram a análise de bots regular usando assinaturas JA3 em suas práticas recomendadas. |

## Fique um passo à frente dos bots maliciosos

Bot Management da Cloudflare

**Implantação simples**
Sem configurações ou manutenções complexas

**Baixa latência**
Latência média de <0,3 ms

**Análises detalhadas**
Correlacione logs de tráfego com outras fontes de dados, como SIEMs ou ferramentas de BI

**Controles precisos**
Ajuste as regras, use um criador de regras visuais ou escreva suas próprias regras de correspondência de padrões

### Pare os bots ruins antes que eles prejudiquem sua empresa

Os bots estão cada vez mais avançados. Há limitações inerentes à detecção e bloqueio de bots à medida que as abordagens dos invasores se tornam mais sofisticadas. As empresas de hoje precisam ajustar constantemente suas estratégias para lidar com a reformulação dos invasores, enquanto alcançam o equilíbrio certo entre segurança forte e minimização do atrito do usuário.

Seja qual for a estratégia que você decida usar, certifique-se de que seu parceiro tenha um conjunto flexível de ferramentas para gerenciar os bots com eficiência. Para saber mais sobre como a Cloudflare pode ajudar você com seus desafios de bots, entre em contato conosco para uma avaliação personalizada.

### Inteligência que você pode confiar

A Cloudflare faz proxy de cerca de 20% de todo o tráfego global da internet o que fornece inteligência em tempo real abrangente sobre comportamentos de bots maliciosos em toda a rede da Cloudflare.
Além disso, a Cloudflare trabalha com vários parceiros que compartilham inteligência sobre credenciais de login roubadas, facilitando a detecção de tentativas de controle de conta antes que resultem em uma violação.

## Comece sua jornada em direção a uma rede mais rápida, mais segura e mais confiável

Solicite uma consulta

**Quer mais tempo antes da avaliação?**

**Continue descobrindo a Cloudflare**