CLOUDFLARE

SOLUTION BRIEF

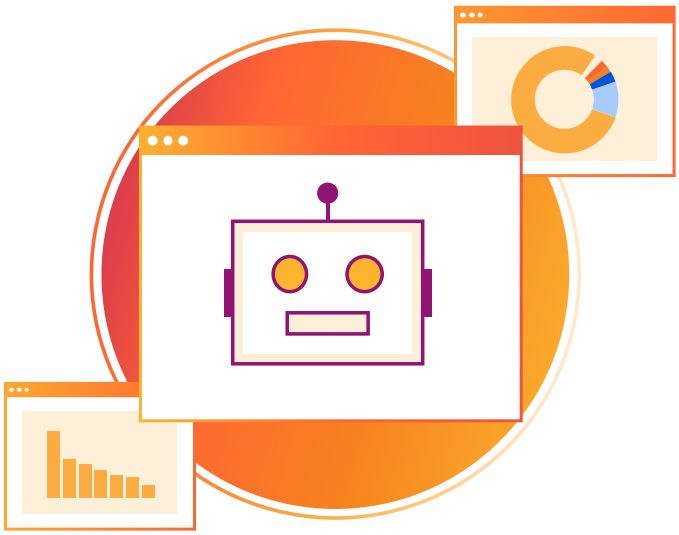
4 Strategies for Managing Malicious Bots

Avoid costly damage and lost revenue from unwanted bots

Bots are everywhere on the Internet

Bots are common on the modern Internet because they help automate important tasks. An estimated 40-50% of total Internet traffic is bot-driven, and many of these bots are performing legitimate business functions.

However, bots are also often used by criminals to attack web properties and cause costly damage. Malicious bots can steal data, break into user accounts, submit junk data through online forms, and perform other malicious activities. These malicious bots waste precious computing and site resources, steal data, and skew traffic analytics.



What is bot management?

Bot management refers to blocking undesired or malicious bot traffic while still allowing useful bots to access web properties. It accomplishes this by detecting bot activity, discerning between desirable and undesirable bot behavior, and identifying the sources of the undesirable activity.

Why is it important?

Bot management is necessary because bots, if left unchecked, can cause massive and costly problems. Organizations need to make sure they aren't blocking necessary bots, like search engine crawling bots, as they attempt to filter out any malicious bot traffic to their web properties.

What can be done?

Identifying and blocking malicious bots before they launch attacks is a critical component of any good security strategy. We've shared four stories of real Cloudflare customers who tackled their bot management challenges with four different strategies using Cloudflare products.

Block the bots

This approach requires care because many legitimate business processes, like search engine indexing, require bots to be able to access company resources.

Block the bots		
Challenge	**Solution**	**Results**
One iGaming company noticed a significant increase in complaints from users. Their accounts were being hacked and credit card information stolen. Malicious actors were using automated bots to brute-force login credentials, gaining access to user accounts and ultimately taking them over.	The security team applied **Rate Limiting** along with advanced **Bot Management** to detect multiple login attempts in a short time. When unusual behavior was detected, rate limiting began automatically blocking malicious requests. Since implementing the rate limiting feature, the iGaming company has not suffered a single credential stuffing attack.	All companies need to balance stringent security with an optimal user experience. The right toolset can help detect and prevent malicious bot traffic while minimizing false positives and hurdles for real users.

Slow down the enemy

This technique maximizes the response time for all suspicious network requests.

Slow down the enemy		
Challenge	**Solution**	**Results**
A sports betting company noticed a significant reduction in transactions. While analyzing the problem, they identified malicious bot activity that was scraping the odds on their website and using that information to gain a competitive advantage.	The company did not block bots because the malicious actors would work around the block. Instead, they slowed down data fetching for betting. They used **Headers Override** to mark suspicious requests based on **Bot Management** analysis, followed by **Workers** scripts to react to these headers and slow down the requests.	This method allowed the company to restore normal user activity. Other methods include using CAPTCHAs for high volume requests or modifying HTML markup at regular intervals. These actions interrupt the bot workflow so that consistent content scraping becomes more complicated.

Deceive the bots

Although many companies deploy bot countermeasures, a truly determined attacker can work around them. Instead, some companies decide to fight back.

Deceive the bots		
Challenge	**Solution**	**Results**
A sports betting company tried to find a solution to bots scraping odds on their website. After some consideration, they decided to launch a workaround with several Cloudflare products that would allow them to feed bots with randomized information.	When the system saw that a request was generated by a malicious bot, it accepted that request and generated a new workflow: Request → **WAF** (bot identified) → **Bot Management** (threat score assigned) → **Workers** (generate randomised data) → **Workers** (return randomized data to bot)	The new workflow generated new randomized data that was returned to the malicious bots. As a result, bots that came to harvest odds and inflict damage went away with something useless, which discouraged any further abuse.

Conduct dynamic analysis

As bots become more sophisticated, companies need to collect data about bots and perform dynamic analysis before taking action. Such goals may include detection of bad registrations, odds, bonus claims, etc. To ensure a thorough analysis, security teams may need to combine multiple data sources from both internal and external tools to analyse parameters of the bot traffic.

Conduct dynamic analysis		
Challenge	**Solution**	**Results**
A betting company launched a marketing campaign to attract new users with rewards for registration. Shortly after launch, they noticed that bots were making fake registrations. The company already had some internal analytics tools, but they didn't give the full picture of bot behavior.	The team implemented Cloudflare's advanced **Bot Management** with JA3 signatures to generate **Raw Logs** of all internet traffic coming to the registration page. They enriched their internal systems with bot scores and JA3 signatures, which allowed them to identify bots more distinctly.	After thorough analysis, the company was able to cancel fake registrations and avoid inflating the statistics of newly acquired users. They introduced regular bot analysis using JA3 signatures into their best practices.

Stay one step ahead of malicious bots

Cloudflare Bot Management

Simple deployment
No complex configuration or maintenance

Low latency
Median latency of <0.3ms

Rich analytics
Correlate traffic logs with other data sources like SIEMs or BI tools

Precise controls
Tune rules, use a visual rule builder, or write your own pattern-matching rules

Stop bad bots before they harm your business

Bots are getting more advanced every day. There are inherent limitations to bot detection and blocking as attacker approaches become more sophisticated. Today's companies need to constantly adjust their strategies to deal with attackers retooling, while achieving the right balance between strong security and minimizing user friction.

Whatever strategy you decide to use, make sure that your partner has a flexible set of tools in place to manage bots effectively. To learn more about how Cloudflare can help you with your bot challenges, contact us for a personalized assessment.

Intelligence you can trust

Cloudflare proxies around 20% of all global internet traffic, which provides extensive real-time intelligence of malicious bot behaviors across the Cloudflare network. Additionally, Cloudflare works with multiple partners that share intelligence on stolen login credentials, making it easier to detect account takeover attempts before they result in a breach.

Start your journey to a faster, more reliable, more secure network

Request a consultation

Not ready for your assessment?

Keep learning more about Cloudflare