Cloudflare Bot Management for Ecommerce

Predict and prevent credential stuffing bots by drawing on worldwide threat intelligence — and safeguard shoppers' trust in your brand.

Bots account for over 40 percent of traffic on ecommerce sites worldwide, and many of them have malicious goals. These malicious bots are becoming more sophisticated by the day, and can mimic the behavior of human shoppers by hijacking real users' browsers and tokens. Some even imitate the helpful search-engine bots that crawl your site and calculate your PageRank.

The most effective way to protect yourself from bot-related fraud — and the resulting lost revenue and damaged customer relationships — is to adopt an intelligent solution that accurately predicts bot attacks before they reach your site.

Why Bot Management Matters for Ecommerce Companies

Prevent theft of website data

Bots can "scrape" pricing information of the inventory from your website — then re-host that same information on a site they control. This can enable competitors' sites to outrank you in search results.

Save on lost revenue and customer compensation

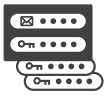
Bots can hoard your inventory, keeping customers from being able to make purchases. And if a bot takes over a real customer's account and makes fraudulent transactions, your could end up having to compensate the defrauded customer. Those costs can add up to millions of dollars every year.

Preserve Brand Trust

When other customers lose faith and trust in a hijacked brand, they'll simply take their business elsewhere. Defrauded customers may even go public with their stories on social media, or report it to news outlets. A public bot-related scandal can significantly degrade trust in your brand for years to come.

Top Bot Problems Cloudflare Solves

While bot tactics targeting travel companies take many forms, these are some of the most widespread:



Credential stuffing, in which a bot takes over a user's account by automatically applying previously stolen account credentials. These fake accounts can then be used to make fraudulent transactions or steal Personally Identifiable Information (PII), which is later sold on the dark web.

Inventory hoarding, in which bots repeatedly add products to their shopping carts but never complete a purchase. This tactic locks up your inventory, preventing you from making sales to real customers. As a result, your revenue and your user experience suffer, potentially drawing negative attention to your brand in the news and on social media.

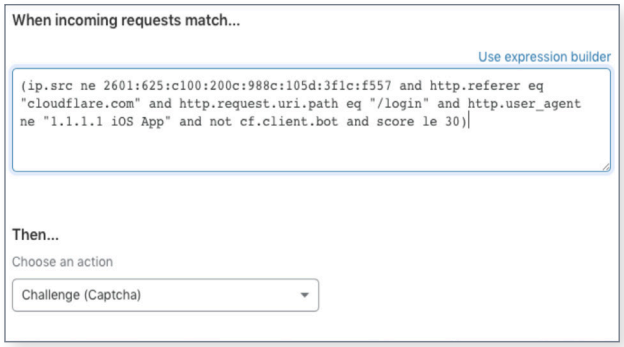
Content scraping, in which bots automatically pull product listings from your site, then re-host that same information elsewhere. Often done for competitive purposes. This can boost the search ranking of your competitors' sites.

REV: 200302

Key Features

SIMPLE DEPLOYMENT

With a single click, deploy a fast and accurate bot management solution without complex configuration or maintenance.

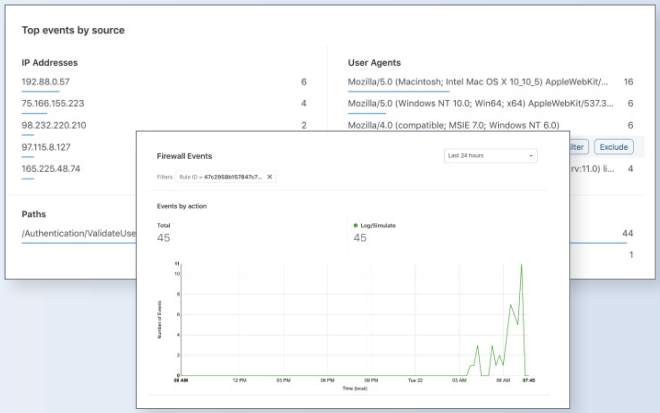


CONTROL AND CONFIGURABILITY

Tune your bot management rules to fit your specific and changing needs. Define the rules with different attributes such as: specific path or URI pattern, request method, score sensitivities. Create tailored mitigation methods, including log, Captcha, block, or alternative content.

RICH ANALYTICS AND LOGS

Get insights with dashboard analytics that help you to improve the solution's effectiveness through time-series graphs with drill-down views. Logs include which rules were triggered, what actions were taken, and rich request meta-data for every request so you can analyze your security posture with third-party tools such as SIEMs or business intelligence applications.



The Cloudflare Difference

Without the right tools, managing bots can become a draining, costly exercise. Cloudflare Bot Management has three key differences:

Threat Intelligence At-Scale

Accurately identify bots by applying behavioral analysis, machine learning and fingerprinting to a diverse and vast volume of globally distributed data.

Integrated Security and Performance

Cloudflare's Bot Management solution seamlessly integrates with its WAF, DDoS and CDN products - enhancing security, user experience, and performance.

Completeness Without Complexity

Instant deployment and protection against a full range of bot attacks without Javascript injection and mobile SDK.