# Cloudflare Bot Management

Detect and mitigate credential stuffing bots by leveraging intelligence from over 20 million Internet properties. All with one click.

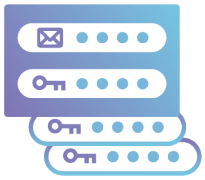
As bots continue to grow in power and sophistication, they are evading traditional defenses.

The potential damage from these increasingly malicious bots includes: breaching sensitive data, stealing SEO traffic by scraping content, disrupting operations, distracting engineering and IT teams from valuable and time-critical work, and damaging the company's brand by impersonating sites or selling proprietary content.

The best defense against bots is data. Not just any data. To combat these bots, you need to leverage data that has both high volume and high diversity to learn from the many different types of attacks before they hit your site.

## Top Bot Problems Cloudflare Solves

A wide range of companies — from e-commerce, SaaS, marketplaces, financial services, and travel/hospitality sites — suffer from bots. The top bot attacks include:



**Credential Stuffing**


**Content Scraping**

**Content Spam**

**Credit Card Stuffing**

**Inventory Hoarding**

## Cloudflare Bot Management

Cloudflare Bot Management applies automated, data-driven approaches to managing bots. This eliminates the manual configuration, investigation, remediation, and deployment steps companies often undertake to address bot problems.

By applying machine learning to a curated subset of traffic across 20 million Internet properties, Cloudflare scores every request for its likelihood of coming from a bot. This large and diverse data set improves accuracy, reducing false positives while protecting your site.

The solution also applies behavioral analysis to detect anomalies in site-specific traffic, evaluating every request on how different it is from the baseline.

Because not all bots are bad, the solution automatically maintains and updates a white list of "good" bots, such as those belonging to search engines.

## The Cloudflare Difference

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

### Smart Data

Learns from a curated subset of traffic to 20 million Internet properties to accurately and proactively identify bots through machine learning and behavioral analysis.

### Integrated Security Services

Cloudflare Bot Management is best-in-class both as a standalone solution and as integrated with WAF and DDoS protection.

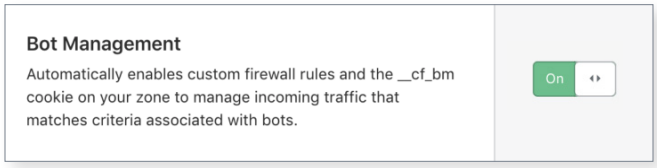
### Completeness Without Complexity

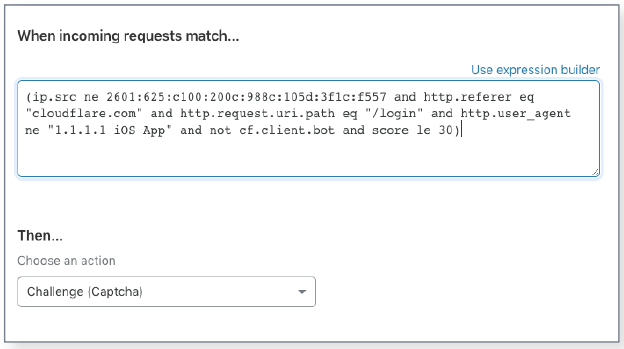
Deploys a bot management solution against a full range of bot attacks with a single click. No JavaScript required.

## Key Features

### ONE-CLICK 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.


## Benefits of Automated, Data-Driven Bot Management

- **Protect revenue and customer trust** by preventing bots from disrupting your business model.
- **Reduce the complexity of threat detection** and intervention by leveraging automation that uses data from one of the largest networks in the world.
- **Keep applications fast and available** by mitigating resource-draining malicious traffic.
- **Improve data integrity** for teams that rely on accurate traffic to run the business.