CLOUDFLARE

PRODUCT BRIEF

Cloudflare Bot Management

Stop malicious bots and manage AI bots with no CAPTCHAs required.

Bots hide in your traffic. Malicious bots hurt revenue and UX.

30% of application traffic on the Internet is automated traffic[1]. Traditional defenses like geography- and IP-based heuristics, as well as CAPTCHA challenges, are easily bypassed by modern bots. These frustrate real users, a lot.

With visibility into **~20%** of the web, nobody fingerprints more AI crawler and search bots than Cloudflare.[2].

Cloudflare Bot Management helps organizations manage AI crawlers and bot traffic to web and mobile apps without CAPTCHAs. Allow verified bots and compliant AI crawlers into apps, while challenging and stopping non-compliant AI bots and malicious bots. This is a key capability in our Application Security portfolio.

Product benefits

- Protect from fraud, financial loss, and brand damage
- Deliver better web and mobile app experiences
- Gain independence from unwanted AI crawlers and search bots

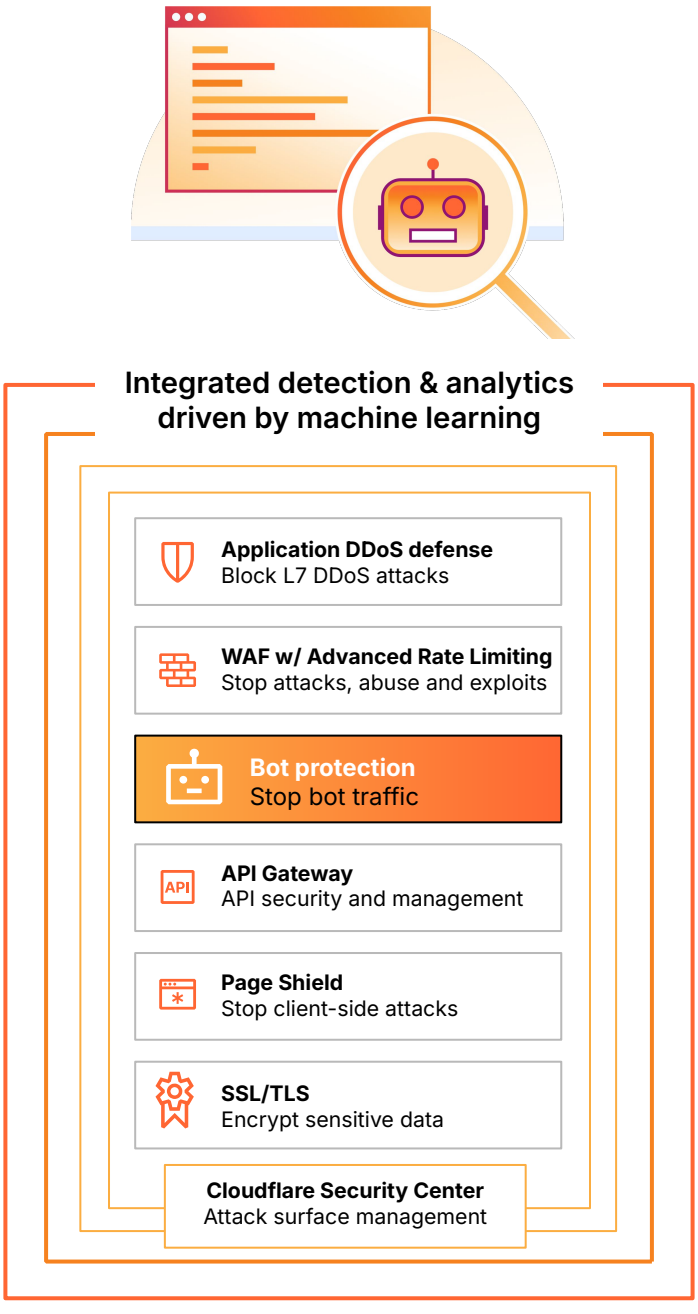

Figure 1: Cloudflare Bot Management integrated within our Application Security portfolio

Sources

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

How Cloudflare Bot Management works

Cloudflare combines multi-layered detection from global and app-specific machine learning, client-side JavaScript, mobile devices, and heuristics in a single bot score that is given to every HTTP request. A bot score indicates how likely that request came from a bot. This bot score is used for standard responses such as block or allow, and for custom response policies via other Cloudflare products. Bot analytics including bot score, HTTP request metadata, and others are available in the Cloudflare dashboard UI or via Cloudflare API in 3rd party tools.

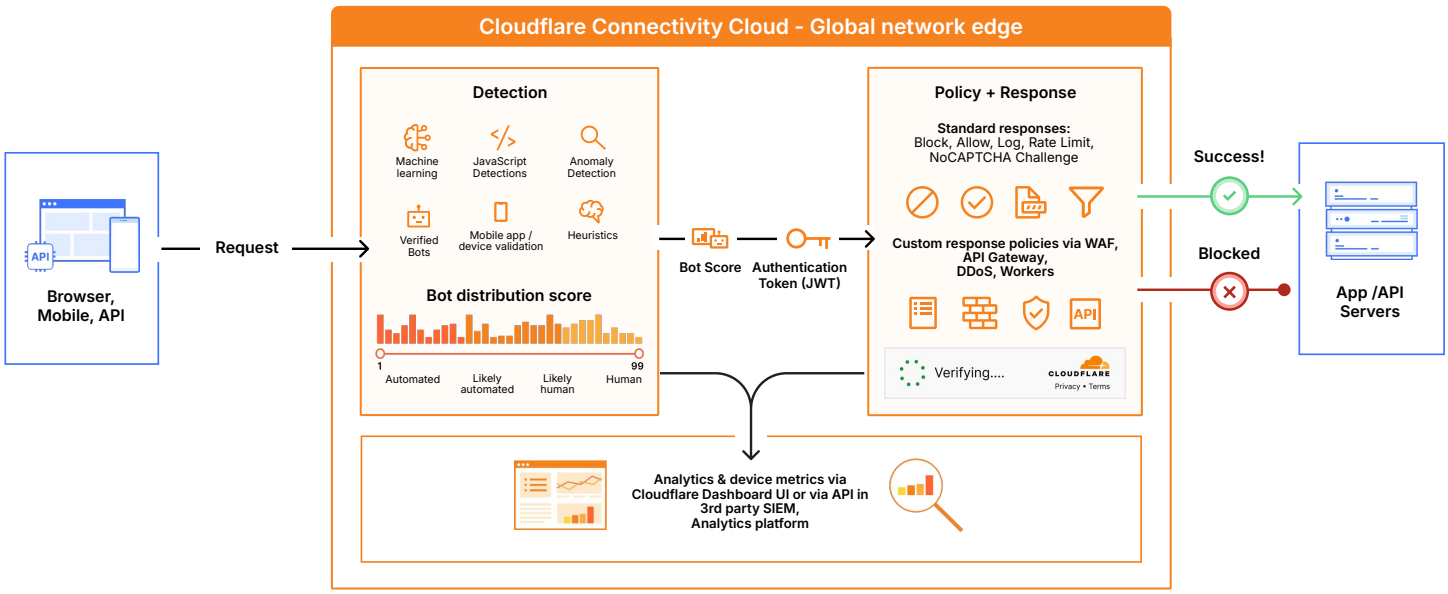

Figure 2: Sample request path through Cloudflare Bot Management

Cloudflare Bot Management key capabilities

Account takeovers and abuse

Protect against zero-day attacks with ML-backed models that can detect vulnerabilities faster than public disclosure. Defend against record-breaking DDoS attacks, protect sensitive data, reduce client-side risks, and monitor your web application's software supply chain.

Defend against bots and fraud

Protect your users from account takeovers and stop bad bots that affect end user experience. Stop malicious botnets, credential and card stuffing, content scraping, and inventory hoarding by combining ML models with client, network, and threat intelligence.

Manage AI crawlers and bots

Exercise stronger control over content and costs by blocking AI crawlers, charging them, or trapping them in never-ending loops. Gain visibility over request patterns and compliance with your robots.txt directives. Available for all Cloudflare customers.

Key Capabilities	
Detection engines	
Machine learning	Our global machine learning model is trained on the entire Cloudflare's global network traffic, which proxies billions of requests daily, to identify automated and human traffic. This is included in our overall Bot Score. Customers are automatically updated to the latest model.
Anomaly detection	Our unsupervised learning behavioral anomaly models baseline application specific traffic patterns and calibrate rule thresholds to identify anomalous bot behavior as customers' traffic patterns change over time. This is included in our overall Bot Score.
Heuristics	We use known patterns of bad bot behavior from previous bot traffic to identify bots. We are regularly updating our heuristics for all customers. This is included in our overall Bot Score.
Verified bots & AI bots	Our bot directory identifies known bot detection IDs that perform legitimate functions and operate transparently as verified bots, as prescribed by Cloudflare verified bots policy. We have a separate category for known AI bots, which may or may not respect robots.txt and hide their behavior from your apps.
JavaScript detection	JavaScript detection module identifies headless browsers and other malicious fingerprints via a lightweight, invisible JavaScript injection on the client side of any request. We honor very strict privacy standards and do not collect any personally identifiable information during the process.
Bot score	Use bot score to write fewer rules to catch majority of bots instead of writing a rule for each bot ID or type. Bot score combines intelligence from our detection engines to produce a score from 1 to 99 that indicates how likely that request came from a bot. A score of 1 refers to definitely automated requests, and 99 refers to definitely human requests.
Device validation via mobile device SDKs	These SDKs for all major mobile app platforms including Android, iOS, React Native, Unity and more validate app integrity, detect unsafe environments, and authenticate API traffic (with self-provided or Cloudflare-approved cryptographic tokens).
Policy and Response	
Standard responses	Setup Block, Allow, Log, Rate Limit, or a variety of user-friendly challenges as responses to bot traffic identified by our detection engines.
Custom response policies	Incorporate Bot Management signals into policies in other Cloudflare products such as Cloudflare WAF, DDoS and write custom actions via Workers.
Analytics	
Cloudflare dashboard	Review bot activity up to 30 days back and filter on bot score and other bot, traffic, and request filters. The bot feedback loop allows customers to report back to Cloudflare any false positives or false negatives for further investigation.
3rd party tools (SIEM, data lake, analytics tools etc)	Analyze Bot Management signals across all your apps in one dashboard via Cloudflare Security Analytics, explore additional log data in Log Explorer, and combine third-party data with Cloudflare data in third-party SIEM or analytics platform via Log Push.

Ready to see more? Register for our App Security Demo Series.