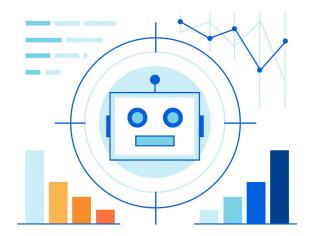CLOUDFLARE®

Cloudflare Bot Management

World-class bot protection from Cloudflare ensures uninterrupted business and lightning-fast web performance.

Cloudflare Bot Management ensures amazing web experiences for visitors. It stops bots from performing credential and credit card stuffing, inventory hoarding, and price scraping, while freeing up security teams to focus on other projects.

Bot Management is part of Cloudflare's application security portfolio. The portfolio also protects APIs, thwarts DDoS attacks, and monitors for malicious payloads and supply chain attacks.

Our application security products work closely with our performance suite, all delivered by the world's most connected global cloud platform.

The most innovative bot detection technology

Cloudflare Bot Management offers granular bot visibility and improves by the minute. Our network sees 25+ million HTTP requests per second; we use this data to conduct active machine learning and fingerprinting.

Detailed bot visibility

Bot Analytics delivers insight into bot patterns and abuse. Segment traffic by a number of different attributes, including bot score, detection engine, and other fields like IP address or user agent.

Layered bot defenses

We detect bots with five complementary detection engines: Heuristics, Machine Learning, Anomaly Detection, JavaScript Detections, and an allowlist for good bots. Cloudflare dynamically chooses the best engine for each request.

Intelligent challenge and response platform

Our response capabilities are dynamic: verify requests as legitimate while frustrating bad bots with fake content. Organizations decide when CAPTCHA or JavaScript challenges are presented, based on Bot Analytics.

Mobile API traffic support

Cloudflare draws on specialized API abuse detections to discern malicious bots from legitimate mobile traffic headed to APIs. We do this without a mobile SDK so as not to impose development burdens on organizations.

Bots never stop harming business

On any given day, bots make up roughly 50% of Internet traffic. Attackers automate bots to operate day and night — they carry out attacks that slow down web properties, or even knock them offline and undermine business.

Credential stuffing/account takeover

Credential stuffing attacks attempt log-ins using stolen credentials, under the assumption the same passwords are used across many sites. This can become account takeover.

Price and content scraping

Bots set up by competitors will scrape pricing data or even steal valuable content (used to undercut your business).

Inventory hoarding

Bots also hoard inventory, when they snap up low-inventory, highly sought-after merchandise in seconds, as soon as it is released, leaving real customers furious.

Content spam

Content and spam bots scrape contact information, create fake user accounts, and fill out marketing forms with dummy data.

World-class application security

The most precise protection

Always thread the needle between security and business with precise protections against bots and attacks. Cloudflare has been tested and tuned for the largest businesses.

Vast integrated capability

No slapdash acquisition code bases thrown together. Rather, integrated security, from a single console, constantly sharpening its threat stopping ability. Performance like CDN, DNS, and traffic acceleration is all built in.

Comprehensive security postures

We deliver full, enterprise-ready, cost-effective security capabilities. We'll never bleed you dry with limited base offerings requiring expensive add-ons or 3rd party marketplace integrations for a strong security posture.

Gartner
peerinsights

customers' choice
2021 ™

Cloudflare Leadership

Organizations gain a more effective application security posture with the Cloudflare global network as their enterprise security perimeter. The Cloudflare application security portfolio has received numerous accolades for its strength and breadth. Gartner named the Cloudflare WAF a 2021 Customer's Choice. Frost & Sullivan recognized Cloudflare an Innovation Leader in Global Holistic Web Protection while IDC and Forrester named us as the DDoS leader.