Bot detection engines

Heuristics

The **Heuristics** engine processes all requests. Cloudflare conducts a number of heuristic checks to identify automated traffic, and requests are matched against a growing database of malicious fingerprints.

JavaScript detections

The **JavaScript Detections (JSD)** engine identifies headless browsers and other malicious fingerprints. This engine performs a lightweight, invisible JavaScript injection on the client side of any request while honoring our strict privacy standards ↗. We do not collect any personally identifiable information during the process. The JSD engine either blocks, challenges, or passes requests to other engines.

JSD is completely optional. To adjust your settings, configure Super Bot Fight Mode from **Security** > **Bots**.

Machine Learning (Business and Enterprise)

The **Machine Learning (ML)** engine accounts for the majority of all detections, distinguishing between human and bot traffic. This approach leverages our global network, which proxies billions of requests daily, to identify both automated and human traffic.

The ML system uses a supervised machine learning methodology to determine the final Bot Score (1–99).

The core model relies on the following process:

- Input Variables (X): Various request features (headers, session characteristics, and browser signals) collected from traffic across the Cloudflare network.
- Output Variable (Y): The predicted probability that a client is human (such as the probability of successfully solving a Challenge). This probability is mapped to the final 1–99 Bot Score.

We constantly train the ML engine on a periodic basis using vast, anonymized data to ensure it remains accurate and adapts to new threats. Customers can analyze the request features used by these models via their own logs, such as Cloudflare Logpull or Logpush.

The ML engine identifies *likely automated* traffic.

Anomaly detection (Enterprise)

The **Anomaly Detection (AD)** engine is an optional detection engine that uses a form of unsupervised learning. Cloudflare records a baseline of your domain's traffic and uses the baseline to intelligently detect outlier requests. This approach is user agent-agnostic and can be turned on or off by your account team.

Cloudflare does not recommend AD for domains that use Cloudflare for SaaS or expect large amounts of API traffic. The AD engine immediately gives automated requests a score of one.

Notes on detection

Cloudflare uses the `__cf_bm cookie` to smooth out the bot score and reduce false positives for actual user sessions.

The Bot Management cookie measures a single user's request pattern and applies it to the machine learning data to generate a reliable bot score for all of that user's requests.

For more details, refer to Cloudflare Cookies.

You can disable the `__cf_bm` cookie using the `bm_cookie_enabled` field via the API.

Previous
← Bot Feedback Loop

Next
JA3/JA4 fingerprint →

Last updated: Aug 20, 2025