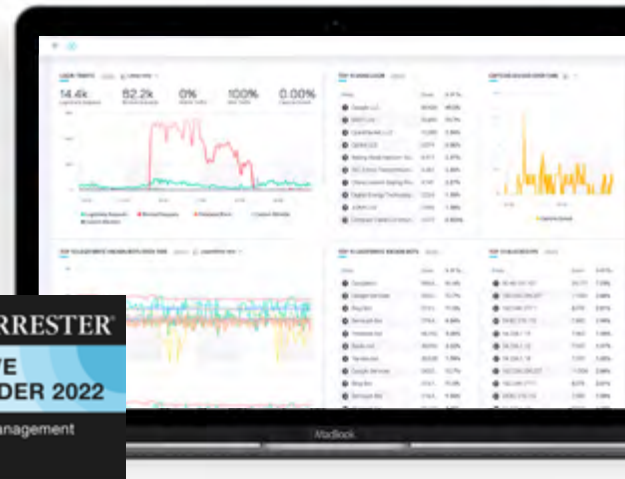




HUMAN Bot Defender: Architected for Low-latency



Stop bad bots without impacting application performance

HUMAN Bot Defender is architected to minimize the impact on website performance by focusing on low-latency techniques. It is architecture-agnostic and deploys out-of-band, meaning it integrates with the customer’s current web technology stack and/or CDN, without the need for any additional tiers or layers.

Human Defense Platform Components

Here is a breakdown of the user session flow within the different components of the Human Defense Platform, which powers the Bot Defender Solution.

Sensor

The Sensor collects and sends anonymized behavioral data from the user’s device/browser

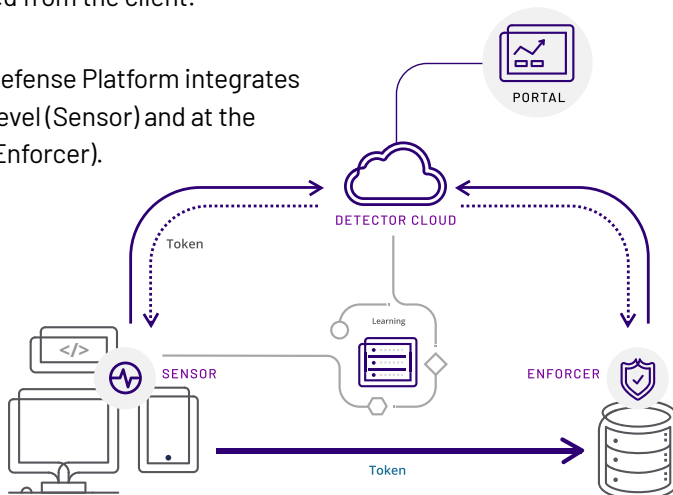
Detector

The Detector processes the data sent from the Sensor to produce a risk score which is sent back as a token to the Sensor. The token is sent to the Enforcer as part of the user session.

Enforcer

The Enforcer enforces the Detector’s decision embedded within the token received from the client.

The Human Defense Platform integrates at the client level (Sensor) and at the server level (Enforcer).



“We seamlessly integrated Bot Defender at our platform edge to ensure maximum protection against automated bot attacks, but also to minimize latency.”

— Alan Murray, Senior Director, Architecture at FanDuel

Sensor size

~70KB

dependent on enabled capabilities/products

95th percentile of API request time

35-50ms

(impacting only 5% or less of legitimate users’ requests)

CPU block time (sync load)

50ms (95th percentile)

Token validation

(impact on user’s request time)

under 2ms (95th percentile)

Client-side Sensor

The client-side component is a lightweight JavaScript for web (Web Sensor) and mobile SDK for native apps (Mobile Sensor for iOS and Android), where the token sent is a cookie for the web user and a header for the mobile user.

The Web Sensor is lightweight (~70 kb), cacheable and operates asynchronously to ensure minimal latency for the page load times. The Sensor executes after the DOM-ready event, and most of the Sensor actions run only once per session to limit the performance impact, so the user experience on the website is not affected.

Cloud-based Detector

The cloud-based Detector processes the data sent from the Sensor to produce a risk score, which is sent back as a token to the Sensor. The token is also sent to the Enforcer as part of the user session.

Server-side Enforcer

The Enforcer integrates on the server side. HUMAN supports more than thirty platform-specific integrations to support different CDNs, load balancers, web servers, application tiers, as well as serverless implementations.

Due to the out-of-band detection, most requests from legitimate users will come with a token (about 95% of them). The Enforcer typically completes the token validation within 2 milliseconds and will handle the request based on the action within the token. The out-of-band execution results in zero network overhead for 95 percent of the legitimate users. Almost all of the legitimate requests from a mobile SDK client come with a token and will not need the additional API call.

When a request has no token, the Enforcer makes a synchronous API call to the Detector that is globally replicated to ensure high-availability and low latency. This API call has a 95th percentile value for response times within the range of 35 to 50 milliseconds. It is important to note that the API call is invoked in rare cases for traffic when the token expires, is invalid or missing. This mechanism also fails-open after a set timeout (configurable) in case the API calls fail to complete.

Global Infrastructure Serving Regions Outside of the US and EU

The latency for LATAM and Asia customers is within acceptable ranges. HUMAN adds PoP for the Detector based on customer demand. Currently, the HUMAN PoP for the Detector are located here:

Americas

us-east1 (South Carolina)
us-east4 (Northern Virginia)
us-central1 (Iowa)
us-west1 (Oregon)
us-west2 (California)

Europe

europa-west1 (Belgium)
europa-west3 (Frankfurt)

Asia

Asia-northeast1 (Tokyo)

About HUMAN

HUMAN is a cybersecurity company that protects organizations by disrupting digital fraud and abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN. **To Know Who's Real, visit www.humansecurity.com.**