HUMAN

HUMAN Sightline

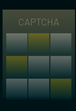
A New Era of Bot Visibility

Simply blocking malicious bots and reporting on volumetric anomalies is no longer enough. Security teams need to know exactly which bots are attacking, how they behave, and what they're trying to accomplish.

Modern bot management solutions must provide granular insights that enable you to maintain a line of sight into attackers as they adapt, so you can respond faster to evolving threats. Here's how bot detection has progressed—and why understanding 'Which bad bot?' is the next step in stopping automated threats.

BOT MANAGEMENT 1.0

Bot or Not?

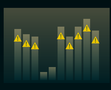


Can detect whether traffic originates from a bot or a human.

CHALLENGE: Does not take into account good bots that you don't want to block or give visibility into bot behavior for nuanced mitigation.

BOT MANAGEMENT 2.0

Good bot or bad bot?

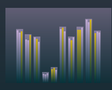


Able to determine whether automated traffic comes from "good" or "bad" bots.

CHALLENGE: Lacks deeper attack context—can flag a bad bot but can't explain its intent, origin, or how it operates over time.

BOT MANAGEMENT 3.0

Which bad bot?



Segments malicious traffic into distinct attack profiles and maps out each one's actions and characteristics.

ADVANTAGE: Provides deep insights into each bot profiles's strategies, methods, and targets over time — and continues to track and block the attacker as it adapts.

Why Knowing 'Which Bad Bot' Matters

Traditional Bot Management: An Aggregate View of Bot Activity

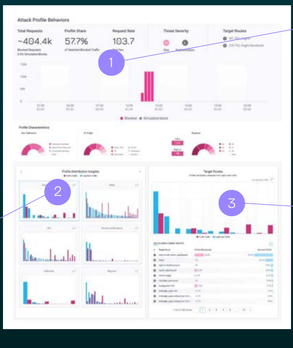
Security teams see only high-level bot activity, such as the top paths visited by all bots. Analysts can't tie specific bots to specific attack paths, forcing them to manually investigate patterns across massive datasets. The only variable to report on is volume, leaving analysts to focus on spikes and potentially miss hidden attacks.

HUMAN Sightline: Deep Insights on Individual Bot Profiles

Bots are segmented into distinct attack profiles using a secondary detection engine that analyzes automated traffic post-decision. Analysts can see which bots visit specific routes, their request characteristics, and actions. This visibility helps assess each profile's behavior, severity, and sophistication—enabling smarter security decisions.

Expand Your Bot Vision with HUMAN Sightline

HUMAN Sightline isolates your automated traffic into distinct attack profiles, so you can uncover in granular detail what each one is doing on your application.



Track the request volume, severity, and timeline of specific attack profiles—so you know which bots are targeting your site, how their behavior evolves, and where to take action.

Compare attack profile characteristics to those of legitimate human users across target routes, IPs, ASNs, devices, browsers, and more.

View the routes and page paths targeted by specific threats, so you can understand attack patterns, detect automation abuse, and respond with precision.

The Business Impact

HUMAN Sightline revolutionizes bot management with AI-driven insights to detect, isolate, and track specific attackers.

Focus and accelerate investigations

See distinct bot activities, paths, and changing behaviors so you can uncover patterns and zero in on attacks, reducing time spent on manual analysis.

Turn bot data into a board-ready narrative

Understand your threat narrative, share business-level visualizations of bot behavior, and show the impact of your team's actions over time.

Make strategic decisions based on specific threats

Gain intelligence on specific attacker actions, define threat priorities, and track and block attacker profiles over time as they adapt.

Powered by Secondary Detection

HUMAN's secondary detection engine uses purpose-built AI to analyze all of your malicious traffic in aggregate after the initial block or allow decision is made. This engine compares every automated request to every other current and past request in order to construct and track attacker "profiles" based on the attackers' characteristics and actions. **Organizations can leverage secondary detection to uncover hidden threat patterns, speed up their investigations, and respond faster** to evolving threats.

Beyond visibility, secondary detection allows HUMAN's detection to **adapt and learn to the attacker's changing behavior.** Now that we can monitor individual profiles over time, the system can react to their specific adaptation, which allows us to continue to track and block the attacker. The number of signatures used by the system for each profile increases over time, and this information is surfaced in the portal.

HUMAN

www.humansecurity.com/platform/features/human-sightline