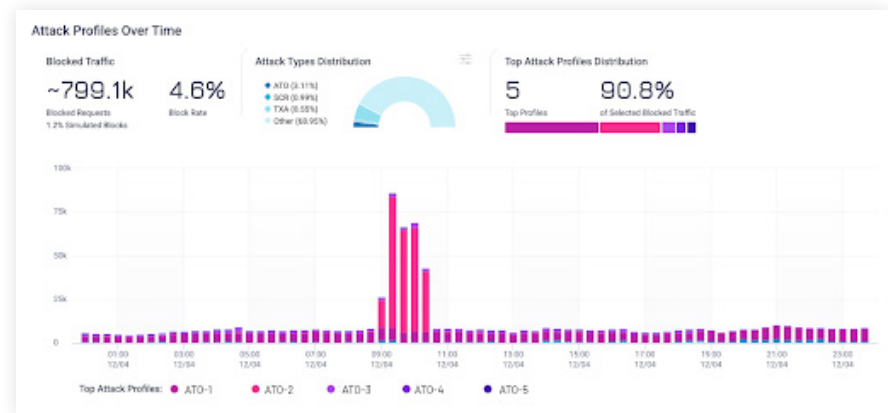# HUMAN Sightline

Get unprecedented visibility into the threats that matter

HUMAN Sightline isolates your automated traffic into distinct bot profiles, so you can uncover in granular detail what each attacker is doing on your specific application. Anomaly detection and signature mapping are not enough to understand your threat narrative. HUMAN Sightline goes far beyond these traditional approaches, offering never-before-seen insights into individual bots' behavior over time.


Benefits

FOCUS AND ACCELERATE INVESTIGATIONS

Turn hours of exploratory analysis into a quick, focused examination of contextualized data. HUMAN Sightline surfaces distinct bot activities, attack paths, and changing behaviors — like bots targeting specific products or visiting select pages. Security teams can uncover hidden patterns and zero in on key attacks, revolutionizing their investigative capabilities.
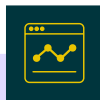
TRANSFORM ATTACK DATA INTO A BOARD-READY THREAT NARRATIVE

Easily tell your bot attack story to key stakeholders and showcase your team's impact. HUMAN Sightline allows teams to present business-level visualizations of bot behavior and show the effect of their actions over time. This empowers security teams to lead with data-backed authority, bridging the gap between deep technical analysis and business actions.

OPTIMIZE YOUR SECURITY STRATEGY FOR YOUR UNIQUE THREATS

Make strategic decisions based on the specific threats you face. With HUMAN Sightline, security teams can gain unprecedented clarity on each attacker's actions and intent, define threat priorities. This real-time adaptability enables security teams to proactively identify new threat patterns, respond faster and stay agile against evolving risks.

How It Works

HUMAN Sightline is powered by our secondary detection engine, which uses layered AI models to compare all current and past traffic on a specific application. It identifies distinct bot profiles based on unique characteristics and attacker actions, going far beyond anomaly detection or signature mapping.

ANALYZE

Purpose built AI algorithms analyze automated traffic data in aggregate after an initial bot-or-not decision is made.

ISOLATE

AI models isolate and segment the automated traffic into distinct bot profiles based on its characteristics and actions.

REPORT

Distinct bot profiles are surfaced in the HUMAN console, with details on their behavior, capabilities and characteristics.

Key Capabilities

Deep Threat Insights
Provides details on attackers' target routes, characteristics, and capabilities, as well as the specific indicators of automated activity, to improve understanding of what exactly happened during an attack.
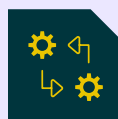
Pattern Analysis
Automatically correlate disparate bot activity to pinpoint bots' strategies, understand the scale of attacks, and identify threat patterns — without sifting through the raw activity data.

Adaptive Learning and Detection
Purpose-built AI models spot nuanced bot behavior shifts as they happen and automatically optimize mitigation workflows based on evolving bot characteristics.
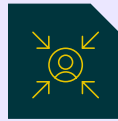
Continuous Tracking Over Time
Tracks bot profiles, including potential AI agents, to ensure a continuous line of sight and continuous protection even as attackers adapt and change tactics.

Bot Indicators and Capabilities
Understand why certain traffic was flagged as a bot and see the specific actions it was taking to evade detection.

Bot vs. Human Traffic Visualizations
Compares characteristics of bot traffic to human traffic (e.g., IPs, ASNs, regions) to help teams visualize the data.

The HUMAN Advantage

Scale

We verify more than 20 trillion digital interactions weekly across 3 billion unique devices providing unrivaled threat telemetry.

Speed

Our Decision Engine examines 2,500+ signals per interaction, connecting disparate data to detect anomalies in mere milliseconds.

Decision Precision

Signals from across the customer journey are analyzed by 400+ algorithms and adaptive machine-learning models to enable high-fidelity decisioning.