

New Cybersecurity Bot Attack Defense Helps SaaS Apps Stay Secure via @sejournal, @martinibuster

Cybersecurity company HUMAN introduces a new feature for its HUMAN Application Protection service called HUMAN Sightline. The new Sightline enables users to defend their SaaS applications with detailed analyses of attacker activities and to track changes in bot behavior. This feature is available as a component of Account Takeover Defense, Scraping Defense, and Transaction Abuse Defense at no additional cost.

Human is a malicious traffic analytics and bot blocking solution that enables analysts to understand what bots and humans are doing and also block them.

According to the Human Sightlines announcement:

“Customers have long asked us to provide advanced anomaly reporting—or, in other words, to mark anomalies that represent distinct attacks. But when we started down that path, we realized that simply labeling spikes would not provide the information that customers really need...

...We built a secondary detection engine using purpose-built AI that analyzes all the 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 “attack profiles,” groups of requests thought to be from the same attacker based on their characteristics and actions.

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."

Search Engine Journal Asked Human About Their Service

How is this solution implemented?

"HUMAN Sightline will be a new dashboard in HUMAN Application Protection. It will be available in Account Takeover Defense, Scraping Defense, and Transaction Abuse Defense, at no additional cost. No other bot management product on the market has similar capabilities to HUMAN Sightline. HUMAN's new attack profiling approach segments malicious traffic into distinct profiles, so customers can identify the different profiles that make up each traffic volume. Analysts can understand what each is doing, their sophistication, their capabilities, and the specific characteristics that distinguish them from other humans and bots on the application. This allows HUMAN to bring attack reporting to the next level, serving as both a bot blocking solution and a data-centric, machine learning-driven analyst tool."

Is it a SaaS solution? Or is it something that lives on a server?

"Our Human Defense Platform safeguards the entire customer journey with high-fidelity decision-making that defends against bots, fraud, and digital threats. HUMAN helps SaaS

platforms provide a safe user journey by preserving high-quality customer interactions across online accounts, applications, and websites.”

Is this aimed at enterprise level businesses? How about universities, are they an end user that can implement this solution?

“This solution is aimed at organizations that are interested in expanding its bot traffic analyzing capabilities. Enterprise level businesses and higher education can certainly utilize this solution; again, it depends how committed the organization is to tracking bot traffic. HUMAN has long been helping clients in the higher education sector from evolving cyber threats, and HUMAN Sightline will only benefit these organizations to protect themselves further.”

Read more about Human Sightline:

Human Sightline: A New Era in Bot Visibility

Featured Image by Shutterstock/AntonKhrupinArt

<https://www.searchenginejournal.com/new-cybersecurity-bot-attack-defense-helps-saas-apps-stay-secure/542403/>