HUMAN Bot Defender on Lumen

Bot mitigation: Stop automated bot attacks

Consumer-facing websites are at greater risk from malicious bots than ever before. Due to the increasing adoption of distributed architectures, the explosion of third-party APIs, and increasingly sophisticated cyber attackers, organizations with digital e-commerce platforms, travel and hospitality sites, or any other application that collects user data have no choice but to prioritize bot mitigation.

Meeting these threats head-on requires a bot risk management solution that is prepared for a wide array of modern attack methods. Credential stuffing, account takeover (ATO), hoarding, and carding are just a few of the schemes that cyber security solutions must be able to thwart. Staying one step ahead of the next threat with a proactive bot risk management solution is key to help ensure that you and your end users are protected.

Stay one step ahead of attackers

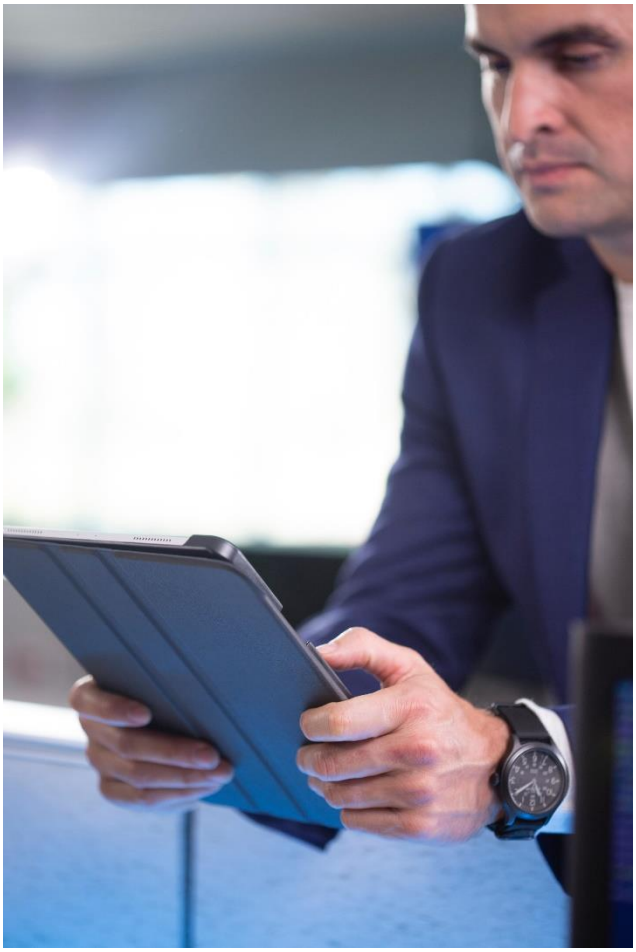
HUMAN Bot Defender uses machine learning and behavior-based analytics to help ensure that your website or application is protected against bots and threats by tracking attack patterns, fingerprinting devices, and monitoring network characteristics to stop attacks at the source.

Rapid, low-maintenance deployment

Pre-integrated into the Lumen global edge, HUMAN Bot Defender can be up and running in a matter of hours without complex development work. Your properties can be protected around the cloud while preserving end-user experience and page response times.

Dedicated security expertise

Rely on the intelligent fingerprinting, behavioral signals and predictive analysis capabilities of HUMAN Bot Defender to detect bots on your web and mobile applications and API endpoints with exceptional accuracy.



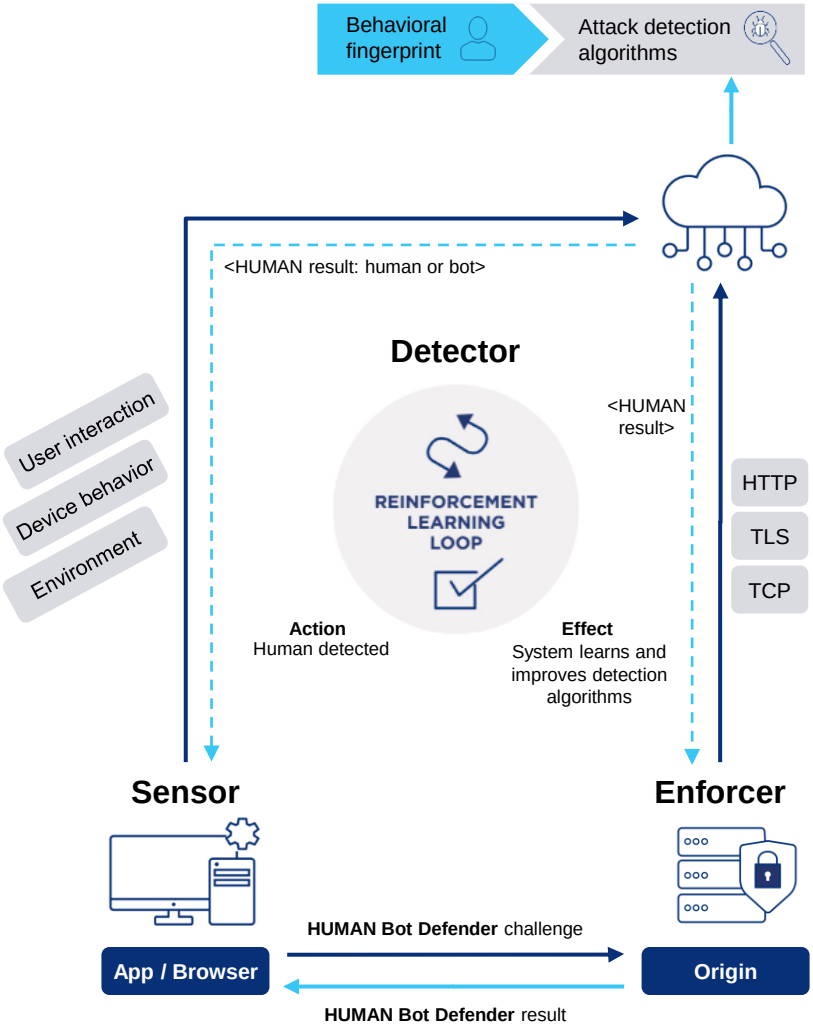
LUMEN®

How it works

Collector: collects and sends hundreds of client-side indicators to the Detector. Signals are used to validate human vs. bot activity, as well as to identify suspicious scripts and malicious browser extensions. The Sensor collects signals asynchronously for the entire portfolio.

Detector: Machine learning-based, the Detector learns common characteristics of human interactions, correlates them with customer-defined policies, and updates the Sensor with new intelligence. It maintains a repository of known attacks shared among all customers. Updates are frequent based on billions of daily data points.

Enforcer: is the gatekeeper for threat response policies generated by the Detector. It enriches and mitigates automated traffic according to business needs. The Enforcer also learns and updates the Detector with relevant data. It can be deployed inline into any existing web architecture.



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. HUMAN was named one of the TIME100 Most Influential Companies of 2023. Protect your digital business with HUMAN. To Know Who's Real, visit www.humansecurity.com.

Why Lumen?

It's all about the experience. Lumen helps enterprises accelerate development workflows, optimize performance, and secure applications through containerized modules designed to power and protect the digital interactions your customer's demand.

HUMAN

lumen.com | application.delivery@lumen.com

LUMEN