HUMAN

HUMAN Sightline Cyberfraud Defense Case Study

Grocery Retailer Identifies Novel Threat with Threat Tracker

This retailer sells grocery items online in the United States and Canada.

Challenge

The grocery retailer experienced automated traffic to their site on a constant basis, including scraping and account takeover attacks. When looked at in aggregate, it was difficult to pinpoint which anomalies to investigate among the noise. The company was looking for a solution to block malicious traffic and streamline their reporting and investigations.

> **“Our site is constantly hit with scraping bots. Normally it’s pretty hard to break through the noise and identify which bot is scraping which pages. By isolating traffic and tying specific bots to their target routes, Threat Tracker helped us identify a new threat that impacted our highly-regulated alcohol sales. We were then able to update our threat models to mitigate this.”**
>
> — Security Architect Lead at Grocery Retailer

Solution

HUMAN was deployed to manage bot traffic, providing the customer with industry-leading protection, advanced reporting capabilities, and deep investigation tools.

ADVANCED BOT PROTECTION

HUMAN delivers best-in-class bot protection using behavioral analysis, machine learning models, and predictive methods to accurately identify 99.99% of malicious bots. The solution also features Human Challenge and Precheck, low-friction, scenario-optimized challenges that enforce additional detections on suspicious requests without impacting the user experience.

SECONDARY DETECTION AND ADAPTIVE LEARNING

HUMAN's secondary detection engine uses layered AI models to analyze automated traffic data in aggregate and identify threat patterns after the initial bot-or-not decision is made. It compares each request with every other current and previous request, identifying hidden threat patterns and automatically optimizing mitigation workflows based on the unique characteristics of fraudulent traffic.

THREAT TRACKER

The Threat Tracker dashboard isolates your automated traffic into distinct bot profiles, so you can uncover in granular detail what each attacker is doing on your specific application. It ties specific bot profiles to their target routes, request characteristics, capabilities, and how they attempted to evade detection. This enables analysts to track threats over time and accelerate their investigations.

Results

With HUMAN, the grocery retailer can block malicious bots with unparalleled accuracy. The company's risk of scraping, account takeover, and carding attacks has decreased, which has a direct impact on their bottom line. Bot mitigation has also improved site performance and saved infrastructure costs. But the benefits do not end there.

Threat Tracker automatically isolates automated traffic into distinct bot profiles, which enables the grocery retailer to tie a specific bot with its target routes. Using this feature, the retailer noticed a scraping bot that was only visiting alcohol pages, which would have remained hidden if they had only looked at scraping traffic in aggregate. The company had not previously accounted for this in their threat model, and this discovery was of great concern as alcohol sales are heavily regulated in the U.S. The retailer updated their threat model accordingly and continued to use Threat Tracker to monitor this scraping bot over time and see the impact of their efforts.

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit ***www.humansecurity.com***