Application Protection Case Study

Global E-commerce Retailer Prevents Account Takeover, Carding Attacks and Review Fraud

This leading global e-commerce retailer distributes vitamins and supplements to customers globally through its website and mobile application.

Challenge

The retailer was experiencing a high volume of malicious bot traffic on their e-commerce portal, including account takeover (ATO), credential stuffing, and carding attacks. The company's security team was working around the clock to respond in real time.

Additionally, fraudsters were also using bots to post fake reviews and 'like' the reviews in order to take advantage of monetary incentives. Not only did this mean that attackers were rewarded for fake reviews, but it also compromised the authenticity of the website's reviews.

> **"When it comes to detection, nobody does it better than HUMAN. They make sure the bots get all the friction without touching the customer experience."**
>
> — Security Engineer, Leading Global E-commerce Retailer

Solution

The retailer needed a solution that would accurately identify and block malicious bot activity without impacting their user experience. HUMAN Application Protection was the clear choice.

PROTECTION AGAINST ATO AND CARDING ATTACKS

With its sophisticated machine learning, Application Protection detects malicious behavior on websites in real time, stopping the most advanced bot attacks.

PRODUCT REVIEW MONITORING

Application Protection applies the same learning techniques to predict when a product review or rating is likely to have been submitted by a bot and challenges the review before it is published.

FLEXIBLE ARCHITECTURE WITH EASY INTEGRATION

Application Protection's open architecture allows it to easily interface with any existing technology stack, including Amazon Web Services (AWS). Application Protection sits in front of the retailer's AWS instances and blocks malicious bot attacks before they reach the servers, without adding an additional layer of in-line traffic processing. This maintains performance and ensures low latency by reducing overall server load. Application Protection also seamlessly integrates with industry-leading CDNs, including Amazon CloudFront with AWS Lambda, to protect services hosted on AWS.

Results

After implementing Application Protection as part of their multi-tier security strategy, the retailer experienced several benefits:

- **Dramatic drop in ATOs** and other malicious bot attacks, ensuring a safe shopping experience without adding friction to the customer journey

- **Significant reduction in fake reviews** being left on the company's product, restoring customers' confidence in using the website's reviews to inform purchasing decisions

- **Improved operational efficiency** because the team no longer had to spend time, money and other resources reactively responding to bot attacks

> "We've seen a significant improvement in our ability to proactively prevent attacks which really takes the pressure off our team. Customer complaints have also decreased now that accounts are secure and we no longer have outages due to spikes in credential stuffing attempts."
>
> — Security Engineer, Leading Global E-commerce Retailer

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