

Account Takeover Defense Case Study

ZALORA Stops Sneaker Bots and Protects Brand Reputation

ZALORA is Asia's leading name in online fashion, beauty, and lifestyle shopping. The company offers over 50,000 products to cover every aspect of the category. ZALORA serves Malaysia, Singapore, Hong Kong, Taiwan, Philippines and Indonesia, carrying an ever-expanding line of local and international brands tailored for consumers in the region.

Challenge

During ZALORA's regular online releases of exclusive new sneakers and clothing, bot operators bombarded the sites with automated attempts to purchase products as quickly as possible. They would then resell the items for inflated prices on secondary markets. ZALORA feared that its excellent reputation with customers would be damaged if its exclusive products were found on other markets.

ZALORA was also experiencing automated credential stuffing attacks, fake account creation, and web scraping. The influx of bad bots created large unpredictable costs and forced the company to scale up its infrastructure. ZALORA needed an advanced bot mitigation solution to handle the increase in sophisticated attacks.

"We were very impressed with how responsive the HUMAN team was to get us this protection and solve our pain before any real damage was done to our reputation. Since then, the product has performed exactly as we expected, accurately stopping bots without any impact on real users. We think we made the right choice in partnering with HUMAN."

— Kenichi Otsuka,
Head of Site Reliability Engineering

Solution

As it became clear that bots were damaging ZALORA's reputation, wasting infrastructure spend, and increasing the company's risk of a breach, the company decided to move their CDN to Amazon CloudFront and then test new bot management solutions. After thoroughly testing three bot detection solutions, ZALORA decided to adopt HUMAN to stop scraping, scalping, and account takeover (ATO) attacks.

ZALORA chose HUMAN because it:



Easily integrates with their CDN provider, Amazon CloudFront, without any code or configuration changes on their origin web servers



Protects against sophisticated bot attacks using behavior-based, machine learning algorithms



Accurately predicts whether a user is a bot before Amazon CloudFront serves a webpage, saving infrastructure costs

Furthermore, the HUMAN support team is available 24/7/365 via Slack, email, or phone to act as an extension of ZALORA's team.

Results

ZALORA deployed HUMAN into their Amazon CloudFront CDN and WAF infrastructure, and they immediately saw a major increase in bot detection. **In fact, HUMAN detected 400% more malicious bots than the previous solution.**

By minimizing bot traffic, HUMAN reduced hosting and bandwidth costs by approximately 30%. This improved site performance and allowed real human customers an honest chance of purchasing exclusive ZALORA products. ZALORA could now stop worrying about brand damage and unplanned infrastructure costs, and could instead concentrate on platform improvements and other core initiatives to drive business growth.

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