CASE STUDY

Global fashion retailer bucks bad bot trends with advanced bot protection

NETACEA

Customer profile

- Global fashion retailer headquartered in London
- 250+ stores and more than 3,000 employees across 26 countries
- eCommerce stores serving North America, Europe and Asia

Results

- Site protected against outages and carding attacks
- Significant server cost savings by blocking scraper traffic
- Prompt and efficient support from bot experts

The challenge

The client is a global fashion brand operating in more than 250 stores worldwide, with eCommerce sites serving the UK, Europe, North America and Asia.

Customer experience is paramount to the brand, driving its recent digital transformation. Ensuring customers are protected against malicious activity online is part of the business' strategy to deliver the best service possible across its eCommerce sites globally.

The organization already had rudimentary bot protection bundled in with another service, but the alarming rise in sophisticated scraping, credential stuffing and carding attacks highlighted the need for a more advanced bot management solution and more specialized support for this issue.

Scraping attacks risk outages at critical moments

The eCommerce site was being heavily targeted by scrapers, acting at scale to collect content and pricing information from across the website. Scraping is the first stage of many potential attack types, including undercutting prices automatically, intellectual property theft, scalping, or even creating a fake website to trick customers and commit fraud.

Aside from these possible attacks, scraping generates a huge number of requests that can be falsely attributed by analytics platforms as genuine traffic, harming business strategy. It also costs money to serve these requests, and there is a risk of slowing the website down or causing outages at critical moments.

Carding attacks targeting the retailer and their payment partners

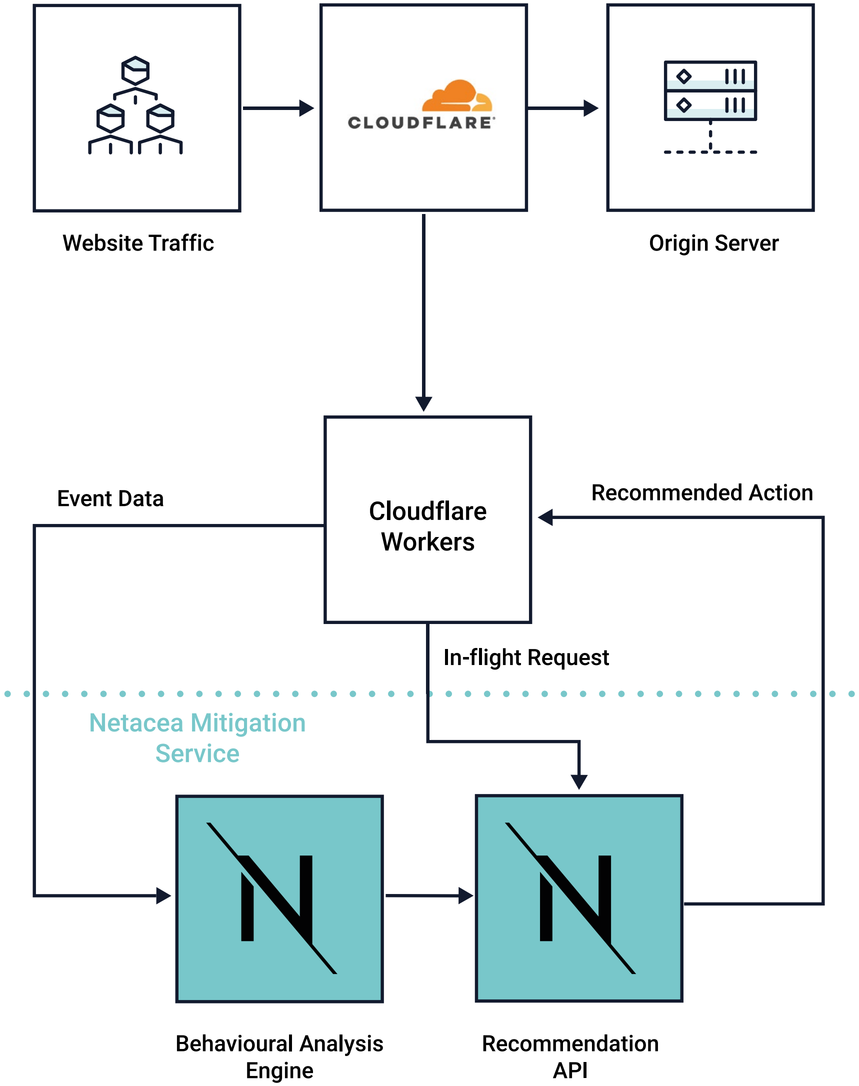
As a prominent online retailer, the business was also concerned about carding (or card cracking), which can generate thousands of requests per second as criminals attempt to validate stolen credit card details. Validated card details may be used to buy higher value goods elsewhere or sold on dark web forums, which is damaging to the card's genuine owner and the business exploited to validate the card, leading to chargebacks, inflated payment processing costs, and tarnished reputation.

The solution

Previously, the organization blocked bots by modifying rules and policies in a reactionary, manual process that spilled out of office hours. With bots quickly bypassing these efforts, the business needed a more proactive and intelligent solution.

Netacea's Intent Analytics® engine goes beyond static rules, instead continually assessing and reassessing visitors with advanced machine learning algorithms in real time to pinpoint known malicious behavior, or flag and cluster together unexpected or anomalous patterns. Combined with analysis from bot experts, Netacea's bot detection service delivers an industry-leading false positive rate of 0.001%.

The organization was quickly able to deploy Netacea Bot Management into its Cloudflare CDN using pre-built Cloudflare Workers and move away from constantly tweaking rules and policies to keep pace with rapidly evolving threats.



The outcome

After working closely with the client to understand its regular and expected traffic and fine-tuning our machine learning models to their use case, Netacea identified aggressive scraping and carding activity on the client's site with a high level of accuracy and confidence.

Example attack overview

- More than 700,000 requests across two attacks
- Bot traffic distributed across 150 countries and 1,000 datacenters
- Offenders hidden amongst normal traffic between attacks

Upon initial investigation, attacks appeared sophisticated. Bots were highly distributed across countries and datacenters, but also disguised their behavior as human; although every attack IP eventually made a request to a specific API endpoint as their final attack goal, they also undertook various other unrelated actions to throw defenses off their scent, such as adding gift cards to their basket, viewing newsletters, and even maintaining a presence on the site at low levels between high volume attacks to look like regular customers.

With this traffic identified and its behavior analyzed, Netacea was able to spot future attacks and prevent them from impacting the business.

The business is now supported by Netacea's bot experts, who are on hand at any time to provide insights into increasingly complex attacks and engineer new solutions to address emerging threats.

About Netacea

Netacea provides an innovative bot management solution that solves the complex problem of malicious bot activity for its customers, in a scalable, agile and intelligent manner, across websites, mobile apps and APIs.

Our Intent Analytics® engine is driven by machine learning to provide an in-depth analysis into all traffic to your site. This gives us an incredibly fast and comprehensive understanding of human and automated traffic behavior, enabling us to identify and block bots in real time with unparalleled accuracy.

With machine learning at the heart of our approach, our technology provides an innovative and profoundly effective solution that is configurable to your environment and adapts to changing threats.