CASE STUDY

NETACEA

Netacea Helps Sneaker Retailer Stop Bot Attacks Missed by CDN Based Solution

Customer profile

- Popular footwear retailer stocking exclusive limited-edition collaborations and brands
- Sneaker bots routinely targeted hot drops to snatch up their inventory for resale
- Used CDN's bundled bot management suite but still affected by attacks

Results

- Netacea detected six times more bot requests than previous solution
- CDN upgraded their package but still fell short of Netacea's detection
- The client now sees significantly less traffic thanks to Netacea blocking bad bots

Six times more bots detected than the previous solution

The challenge

The client is a trend-setting footwear retailer operating two brands, selling some of the most sought-after shoes for labels such as Nike, Adidas and UGG.

Due to the high-demand nature of their products, the retail group is besieged by automated attacks on their eCommerce platforms, as scalpers aim to scoop up the entire inventory in rapid succession to resell at a profit. Bots aggressively scrape product availability information, putting considerable strain on the service at peak times, which caused outages and slowdown whilst incurring significant overage charges for their infrastructure.

Bots then automate the add-to-cart and checkout process, purchasing the whole stock allocation from under the noses of genuine customers in seconds. The scalper groups responsible were boasting online about snatching the hottest releases from the client causing significant reputational damage for the business, from both angry customers and suppliers who had to undertake costly investigations into fraudulent orders.

Although the retailer's CDN had bundled a bot management solution in with their security package, they were fighting a losing battle. This left them frustrated by the need to constantly update blocking rules that were quickly bypassed, and disappointed in their solution's inability to detect and mitigate attacks.

The solution

In an offline proof of value exercise analyzing 28 days' worth of web logs, Netacea identified six times more malicious bots than the CDN's solution had spotted.

In response, the incumbent bot protection supplier upgraded the client's package to their highest tier, but Netacea was still able to detect three times as many bad bots than the incumbent's enhanced solution.

How Netacea beat the existing bot protection solution

Netacea is proven to detect as much as 600% higher levels of malicious traffic than competitors due to our unique bot protection technology and methodology.

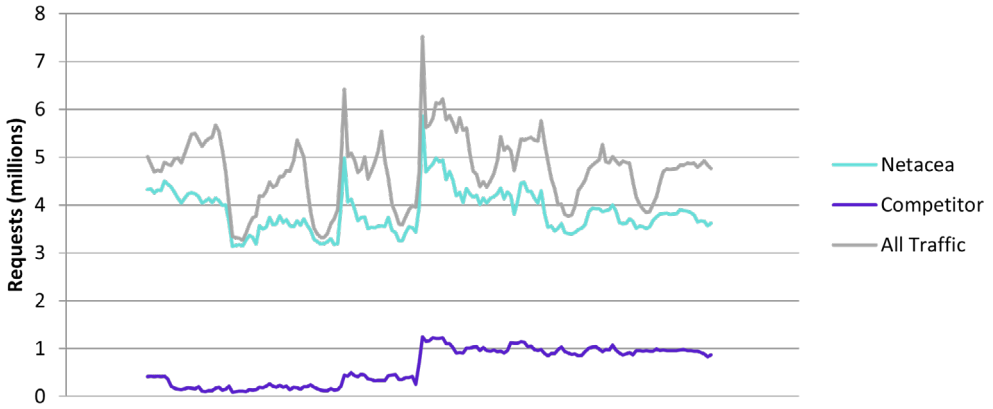
The retailer's previous supplier used rate limiting to block IP addresses making a suspicious number of requests over time. However, sophisticated bot users can bypass rate limiting by distributing the attack across multiple origins.

To combat this, Netacea uses behavioral analysis of all traffic simultaneously. Even when an attack is dispersed across different data centers, countries, IP addresses and using many different user agents, Netacea's machine learning based detection engine can identify and block the bad traffic.

The old supplier also used fixed lists of origins that are either blocked or allowed. As new attackers emerge and old attackers retool, these lists need to be changed constantly, which took hours or sometimes days to implement, leaving the client exposed to zero days whilst requiring complex change control to manage.

With Netacea, changes in attacks are blocked proactively and automatically, with no input required from the client thanks to our machine learning approach and integration at the edge. This saves time and always delivers up-to-date protection.

Malicious traffic detected by Netacea vs old supplier



Integrating with Netacea

The client was able to integrate Netacea Bot Management with their existing CDN very quickly using a ready-made plugin. This allows the client to still benefit from their CDN's WAF and DDoS protection, whilst adding Netacea's superior bot detection capability, adding close to zero latency to the platform with seamless integration.

NETACEA

The outcome

Once the client deployed Netacea's mitigations inline and switched off their previous bot protection supplier, they saw an immediate drop in requests to their platform, with no impact on orders or conversions, indicating a high level of blocking accuracy and very low false positives.

"Netacea has managed to pick up bot threats that other competitors don't even notice due to a great threat detection system."

– Ecommerce Operations Manager

This has reduced the strain on their infrastructure, resulting in a more stable platform with less risk of outages. Netacea's deployment at the edge also means the client doesn't have to spend time updating policies anymore, as detection modules are automatically kept up to date, allowing for faster mitigation of zero days and new bot attacks.

Blocking bad bot traffic also prevents scalpers from snatching popular items for resale, removing frustration for customers and suppliers. Netacea's bot expert team provide actionable insights after product drops, saving time in manual investigations that keep the retailer's suppliers happy too.

Benefits

- Reduced strain on infrastructure
- Scalping prevented during hot drops
- No more slow, manual policy updates to stay protected
- Faster detection of zero days and new bot attacks

About Netacea

Netacea provides an innovative bot management solution that solves the complex problem of scalping, scraping and 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 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.