CASE STUDY

Netacea detects 11 times more bots than previous solution for luxury shoe retailer

Customer profile

- Luxury shoe retailer with revenues over €250 million
- Stocks over 600 iconic brands and hyped releases
- Based in Italy, serving 10 languages with worldwide shipping

Results

- 73% reduction in requests by removing bad bots
- 10% reduction in CPU utilization
- Removed the effectiveness of known sneaker bots

NETACEA

11x more bad bots blocked, reducing web requests by 73%

The client, an Italian shoe retailer with a global online presence, is known for its curated selection of over 600 luxury brands including iconic labels and emerging talents. Their website, available in 10 languages, has over 50 million unique visitors each year, and generates annual revenues exceeding €250 million.

The Challenge

During hype drops of popular brands such as Yeezy and Air Max, the site's traffic increases by 40-50%. The retailer realized that the bulk of this traffic was large volumes of scraping bots making concentrated requests on their website and mobile API. These requests were specifically targeting limited-edition sneaker pages within their catalogue.

The retailer's sought-after range makes it a high-value target for the sneaker bot community, whose goal is to snatch up limited edition shoes as soon as they go on sale and resell them on secondary markets at a huge markup. Netacea's threat research team confirmed that several popular sneaker bots advertise compatibility with the retailer's website.

Attackers use automated programs called scalper bots to snatch as much inventory as possible and maximize their profits. To determine exactly when, where and how to target their scalping attacks, web and API scraping bots constantly query the site for data related to these drops – Prices, sizes, specifications, checkout paths and availability are aggressively scanned by competing groups.

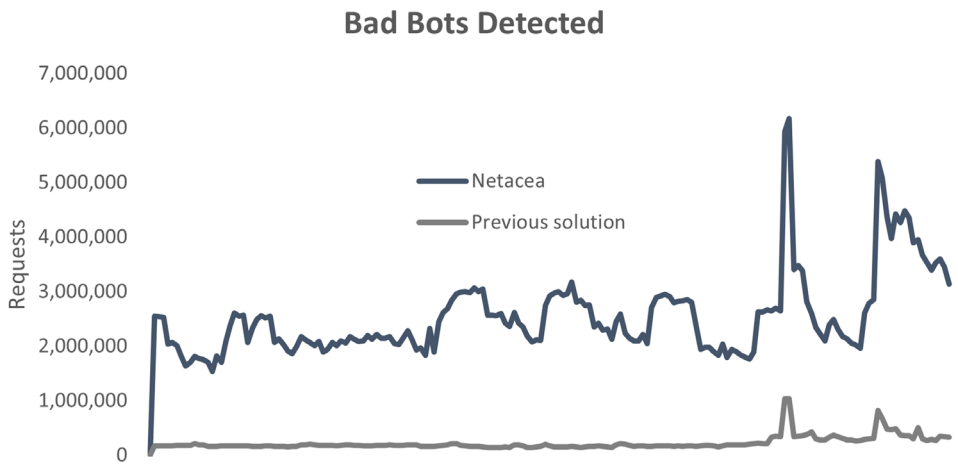
Scraper bots had found ways to bypass the existing bot protection solution and were causing significant strain on the infrastructure, especially during high-profile drops and sales.

This led to slow loading pages, affecting conversion rates on key products, as well as over-spending on infrastructure just to serve traffic to bad bots. In a worst-case scenario, bots were causing outages and loss of website availability.

The solution

Netacea began by investigating live traffic coming to the retailer's website and mobile API using our machine learning-powered Intent Analytics® engine. After analyzing 608 million requests, we identified that bad bots accounted for 457 million – 75.2% of all web traffic. Most of this targeted product pages of popular sneakers, specifically Nike ranges including Air Jordan, Dunk and Air Max, as well as login paths, indicating the early stages of a scalper bot attack.

This traffic was highly distributed across countries, datacenters and IP addresses, pointing towards a sophisticated campaign to bypass existing defenses. This had proved affective to date, as Netacea detected 11 times more traffic than was blocked by the incumbent bot management solution.



How Netacea beat the existing bot protection solution

Compared to Netacea's detection capability, the retailer's existing bot management solution missed a staggering 91.2% of bot attacks. We detected far more malicious traffic thanks to our unique bot protection technology and methodology.

With huge monetary gains at stake, sneaker bots are notoriously advanced and adaptable to defenses. This makes the antiquated tactics employed by the retailer's incumbent bot protection, such as rate limiting suspicious IP addresses, ineffective – sneaker bots routinely distribute their origins across thousands of IP addresses.

We take a different approach, instead using behavioral analysis on the entirety of web traffic to spot malicious activity, wherever it originates. Netacea Bot Management can discern sophisticated bad bots even when spread across many different data centers, countries, IP addresses and user agents.

Unlike the existing bot defense, Netacea requires no manual changing of rules and block lists to keep up with attackers. This is saving the client hours, if not days of effort internally, as the machine learning powered Netacea solution does the work for them and keeps them protected from rapidly adapting bots.

Integrating with Netacea

The client swiftly integrated Netacea Bot Management into their existing CDN by utilizing a pre-built plugin. This integration enabled the client to retain the advantages of their CDN's WAF and DDoS protection, all the while augmenting their capabilities with Netacea's advanced bot detection, seamlessly enhancing the platform with nearly imperceptible latency.

The outcome

Since mitigating bot attacks with Netacea, the client has cut overall requests to their website by 73%. This has reduced their CPU utilization by 10%, opening the door for an overall leaner and more cost-effective infrastructure. This has also made their platform more stable during hype drops of items such as Yeezys and Nikes, leading to a smoother shopping experience for customers.

Since deploying Netacea Bot Management, our threat research team has noticed that support for attacking our client's website has been discontinued by major sneaker bot operators, indicating their modules can no longer bypass defenses. This gives genuine customers a better chance at buying the most desirable brands and items as they are released, improving customer satisfaction, as well as keeping suppliers happy.

As well as better bot blocking, the switch to Netacea has freed the team from manually changing blocking rules in vain, and investigating incidents caused by sneaker bot attacks.

About Netacea

Netacea provides an innovative bot management solution that solves the complex problem of credential stuffing, account takeover and other malicious bot activity for our 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 on 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.