CASE STUDY

Netacea Protects UK's Largest Loyalty Scheme from Bot Attacks

Customer profile

- Top five global retailer
- £60 billion annual turnover
- Loyalty scheme with over 20 million members

Results

- 650,000+ malicious login attempts mitigated per week
- Customer account fraud costs reduced by £1.4m per month
- Internal product and security resources freed up to focus on business needs

NETACEA

£1.4m a month in fraud costs saved for one of Europe's biggest loyalty schemes

The challenge

Our client, one of the world's largest retailers, operates a 20-million-member customer loyalty scheme – the most popular in the UK.

The retailer identified they were frequently suffering credential stuffing attacks, mainly focused on their loyalty points accounts. Using username and password pairs leaked from other sites, attackers were gaining access to the retailer's customer accounts, at which point they could spend, transfer or sell loyalty point balances on the dark web.

These attacks targeted quickly redeemable items like hotel stays, fast food vouchers and shopping gift cards. This allowed attackers to cash out within 48 hours, before their attacks could be identified and the funds cut off.

This cost the retailer millions each month, both in reimbursing defrauded accounts and replenishing items bought with stolen points. Customers were also getting locked out of their accounts, causing frustration on top of losing their points balances, and taking time to restore access.

The volume and sophistication of these attacks, which were being missed by WAF and DDoS protection tools in place, risked causing outages and eating up costly server resources. The business's Security Operations Centre (SOC) team were forced to take manual mitigation measures, putting strain on internal resources. The team needed to move from being reactive to proactive against attacks.

"We had a team of ten people who were having to manually block IP addresses and user agents of credential stuffing attacks that could occur at any time. We had to make the business-critical decision to move to a proactive approach and improve our security."

- Head of Security

The solution

Focused on putting customers at the heart of everything it does, the business decided it needed to take a more proactive approach to protecting customer accounts from credential stuffing attacks, account takeover, and loyalty point fraud.

After running a formal RFP, followed by proof-of-concept engagements with multiple suppliers, Netacea was selected as vendor of choice due to its unique, highly accurate approach to bot identification, the flexibility of implementation and the advanced mitigation options provided.

Netacea integrated its bot management solution into the customer's existing technology stack, pulling data from the SIEM solution and pushing recommendations and actions back via Netacea's API.

Netacea uses advanced AI and a suite of machine learning approaches to detect and mitigate both high-volume and "low and slow" attacks. Our data scientists train supervised machine learning models to instantly identify requests acting maliciously, even if these are distributed across a wide range of origins (countries, data centers, IP addresses, user agents etc.) to avoid detection.

Netacea augments our supervised models with Intent Clustering, which creates dynamic clusters of requests in real time based on visitor behavior. This allows our bot experts to identify malicious requests, which are fed back into our mitigation engine.

If a credential stuffing attack is identified, Netacea sends alerts to the SIEM solution where the retailer can take several actions depending on the risk score assigned to the visitor, including limiting account functionality, requesting further verification, or locking or resetting the account.

NETACEA

The outcome

Netacea accurately detected over 650,000 credential stuffing attacks targeting the site within the first 30 days of engaging. Netacea also highlighted continued low and slow attacks that were flying under the radar of existing tooling.

Netacea's bot management solution enables the retailer to proactively protect more than 20 million customer accounts, both on the website and via their app, and facilitate over 100,000 customer logins every hour without adding any latency or friction to the customer journey.

Working with Netacea, the retailer has realized significant cost savings, with a reduction of £1.4m per month in fraud costs from breached customer accounts.

Alongside fraud savings, Netacea has reduced the strain on the retailer's internal resources. Security and fraud teams are no longer reliant on manual intervention and can focus on other business priorities.

"Netacea helped us successfully make the switch from reactive bot management to proactive identification and mitigation. Netacea has taken the pressure off our internal resources and we now feel confident that our customers' accounts are no longer vulnerable to continual credential stuffing attacks."

– Security Operations Manager

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.