CASE STUDY

Protecting a Growing FinTech Against Credential Stuffing Attacks

Customer profile

- FinTech providing customers with free financial information
- 12 million users throughout the UK, Australia and South Africa
- More than 100 employees at the firm's UK headquarters

Results

- 250,000 credential stuffing attacks stopped every week
- 10 million customer accounts protected
- 5% reduction in traffic to login pages, APIs and apps

NETACEA

The challenge

A fast-growing global FinTech organization was frequently observing large spikes in automated bot traffic on its login pages and APIs.

The business was concerned about the risk the traffic posed to its customers. If left unchecked, the increasing surges in traffic made the organization vulnerable to the very real threat of a data breach that could expose sensitive Personally Identifiable Information (PII) and result in fines from the FCA, while putting the brand at risk of significant reputational damage.

Tackling this traffic put strain on the internal SOC team, which was regularly required to carry out late-night manual blocking of suspicious traffic to minimize the threat to customer accounts.

Sophisticated bots bypass broad defenses

Despite having a WAF and CDN solution in place, the increasing necessity for manual intervention and false positives and negatives in alerts made it abundantly clear that sophisticated bots were continually bypassing traditional security measures.

Managing and maintaining rules and policies had become a game of whack-a-mole, with bots quickly adapting to these defensive measures. This made dealing with the automated traffic internally a time-consuming and unsustainable task. It was determined that the business' incumbent providers did not have the expertise or flexibility to detect sophisticated attacks and a new approach was required.

The solution

Netacea was able to solve these problems by combining our Active Threat Database, which is driven by trillions of assessments across our entire estate, with our Intent Analytics® machine learning engine.

Netacea's bot experts quickly identified that malicious bots were persistently bombarding the FinTech's login page with automated credential stuffing attacks.

The business was quickly able to deploy Netacea Bot Management into its Cloudflare CDN using pre-built Cloudflare Workers.

Benefits of the implementation:

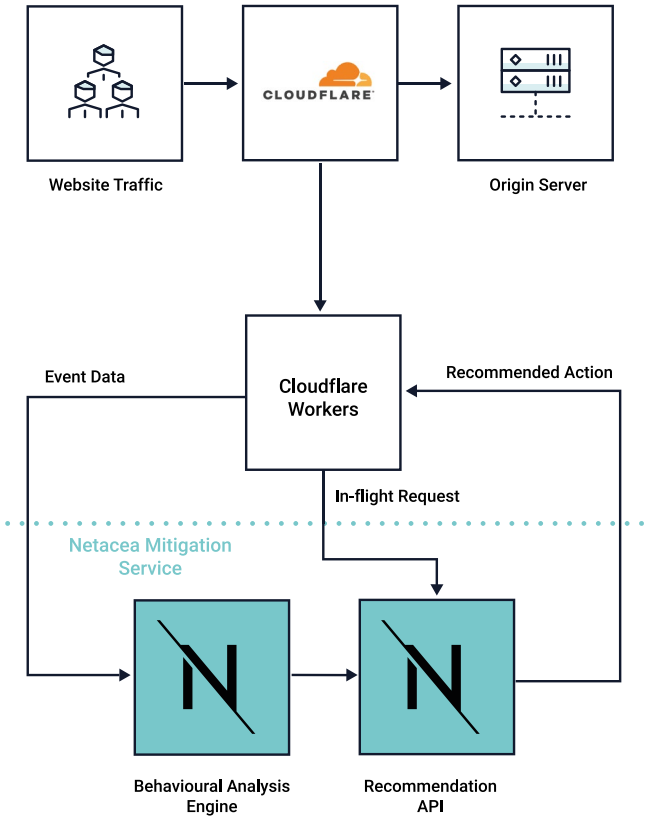
- Automated threat blocking with regular reviews to ensure the most effective mitigation
- Auto-scaling and proactive monitoring means the solution meets demands during peak periods
- No additional latency added to the customer journey

A standard Cloudflare logging endpoint streams access logs to Netacea, with no increase in latency. The mitigation strategy is checked on subsequent requests with minimal (<10ms) additional latency.

The solution is deployed with automatic threat blocking, with internal monitoring tools and regular customer review meetings ensuring that the most effective mitigation strategy is always in place.

Incorporating automatic blocking along with Netacea's auto-scaling and proactive monitoring enables the solution to meet demand during periods of peak usage, taking the pressure off the customer's internal SOC team. Now receiving the continual support of Netacea's Bot Experts team, the SOC team receives:

- Support for management of the solution
- Recommendations made by Netacea's Intent Analytics® engine
- Regular updates on emerging bot threats



The outcome

Once inline, Netacea's dashboards quickly illustrated the extent of the bot attacks and the FinTech's SOC team worked closely with Netacea to build up tailored rules for automated mitigation.

After six months, Netacea is now blocking on average 250,000 credential stuffing attacks per week to deliver the following benefits:

- More than 10 million accounts protected from credential stuffing attacks
- 5% reduction in traffic to login pages, APIs and apps
- Internal resource preserved with teams no longer required to respond to attacks out of hours

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.