CASE STUDY

NETACEA

Protecting “The Big Game” Live Stream from Bot Attacks

Customer profile

- OTT streaming platform with 65m+ subscribers
- $7bn+ annual revenue from subscriptions
- Exclusive streaming rights to American Football’s “Big Game”

Results

- Zero outages caused by bots during major event
- 24 million requests analyzed
- 35% of API login attempts flagged as malicious and blocked
- 0.0001% false positive rate

Zero outages caused by bots during “The Big Game”

0.0001% false positive rate

The Challenge

Our client, a major US video streaming platform, had exclusive rights to air American Football’s “Big Game” in February 2024.

With 120 million people expected to stream the game live, it was vital for the business to ensure uptime and stability of their platform throughout.

However, the business knew that they were at risk from attackers using the high traffic expected during the game to disguise malicious bot attacks, particularly targeting customer accounts.

Automated traffic and credential stuffing attacks could not only compromise their customers, but also the stability of the whole platform.

Because customers use various devices to login and watch, from laptops and mobile phones to smart TVs and games consoles, the client needed a solution that could detect sophisticated malicious traffic disguised within these endpoints.

The customer also needed a lightweight solution that could accurately detect traffic from known bad traffic sources across their entire platform without impacting their infrastructure or operations.

The Solution

Safeguarding login and registration with AI-Powered Bot Protection

Netacea protected the platform against credential stuffing and fake account creation with AI-powered bot protection, analyzing every single login and registration request worldwide across all websites, apps and APIs.

Unlike tools that rely on client-side integrations, which are complex to deploy across multiple platforms, simple to bypass and inadequate for protecting APIs, Netacea plugged straight into the customer's CDN to ingest server logs into our Intent Analytics® engine.

This data was analyzed using specifically tuned machine learning models so sophisticated attacks could be blocked with confidence in near real-time.

We also provided support both on-site and remotely to the client, ensuring they had immediate answers to any questions and reassurance of the efficacy of the Netacea solution at this crucial time.

Blocking known bad traffic across the entire platform with Bot Threat Feed

To keep known offenders away from their entire platform throughout this key event, the customer also integrated the Netacea Bot Threat Feed directly into their CDN.

Netacea Bot Threat Feed is a large dynamic dataset of known malicious traffic sources, collected across the billions of requests Netacea's AI bot protection solution analyzes daily across our entire customer network. We verify and add over half a million previously unseen attack sources to the feed daily.

By using a lightweight, simple to manage integration into their security stack, the customer protected their entire platform against verified bad actors at the point of entry without manual intervention.

The Outcome

During the lead-up, the game itself, and its aftermath, Netacea Bot Protection automatically blocked five million malicious requests attempting to access accounts or register new ones.

False positives were incredibly low (0.0001%) meaning that genuine customers were unaffected by our highly accurate mitigations.

Around 35% of all requests to the authentication API were malicious bots, with over a million disguised as requests from Xbox consoles. As credential stuffing attacks are successful in roughly 0.1% of attempts, inadequate protection from solutions unable to monitor APIs natively could have allowed criminals to steal 1,000 accounts in this instance.

During the game, the streaming platform was also targeted by several highly volumetric attacks to other areas of their system, rapidly dwarfing their expected requests per second several times over.

With Netacea Bot Threat Feed recommendations active, they were able to identify these traffic surges as coming from known malicious actors and prevented them from reaching their critical infrastructure.

This allowed them to focus on serving real users across the entire platform during their peak time of the "Big Game" without need for manual interventions from the security or infrastructure teams.

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.

NETACEA