Case Study

# Protecting "The Big Game" Live Stream from Bot Attacks

## Highlights

**100%** Availability for customers during the "Big Game"

**99.99%** Mitigation accuracy

## Customer Profile

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

## Results

- Maintained reputation - Happy customers during biggest event of the year
- 100% availability during the event
- Nullified the attack threat site-wide using Netacea Bot Threat Intel
- We did this without impacting customers (0.001% false positive rate)

## The Challenge

Our client, a major US video streaming platform, held exclusive rights to air American Football's "Big Game" in February 2024.

With 120 million viewers expected to stream live, this was a huge commercial opportunity - but also a major risk. Attackers were likely to exploit the surge in traffic to mask an exponential increase in malicious bot activity, particularly targeting customer accounts.

Without the right protection, these threats wouldn't just impact platform stability - they'd limit the platform's ability to fully monetise the event.

Automated traffic and credential stuffing attacks risked compromising both customer accounts and platform stability. With bots exploiting promotional offers, the platform couldn't fully capitalise on a major growth opportunity.

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.

NETACEA

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

STEP 01

### Safeguarding login and registration with AI-Powered Bot Protection

Netacea ensured the platform could protect itself 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 real-time.

Our industry-leading support team were there right when the client needed us, on-site with the teams running the event, liasing with other third parties.

STEP 02

### Defense in Depth with the Bot Threat Feed

To deliver true defense in depth during this critical event, the customer combined targeted detection and mitigation on their most sensitive user journeys with broad protection from Netacea's Bot Threat Feed (BTF), integrated directly into their CDN.

The Bot Threat Feed is a large, continuously updated dataset of known malicious traffic sources. It's built from billions of requests that Netacea's AI-driven bot protection analyses daily across our global customer network. Over half a million new attack sources are verified and added to the feed every day.

This approach enabled the customer to secure their entire platform: blocking malicious traffic at the edge without manual effort. The Bot Threat Feed also served as an early warning system, highlighting emerging attack types and allowing the customer to adjust their defences in real time as threats evolved throughout the event.

## The Outcome

Netacea stopped five million fake accounts being created, whilst ensuring that no customer accounts were breached.

Around 35% of all requests to the authentication API were malicious bots, with over a million disguised as requests from Xbox consoles.

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's Bot Threat Feed active, the platform automatically blocked traffic surges from known malicious sources: protecting critical infrastructure and allowing the team to focus on real users during peak demand without manual intervention.

## About Netacea

Netacea is a leader in bot management, trusted by global brands to stop credential stuffing, account takeover and other advanced bot threats. Our solution uses machine learning to detect and mitigate malicious activity across websites, mobile apps and APIs: delivering intelligent, scalable protection that evolves with the threat landscape.

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.

See Netacea in action today

Schedule your free demo at Netacea.com

NETACEA