Arkose Labs

Arkose Labs Helps Gaming Giant Stop Automated Attacks and Save Millions of Dollars

CASE STUDY

A Large Gaming Platform

Business Problem

- In-game currency abuse through automated, bot-triggered sessions
- Bot-driven plays on behalf of the others to increase rank and levels
- Account takeover of genuine user accounts to drain/transfer their assets
- Auction house abuse to manipulate in-game economics

Solution

Arkose Labs deployed custom in-game enforcement challenges that accurately filtered out bots and organized sweatshop attacks enabling the client to prevent fraud while delivering a seamless user experience

Results

- Fifteen-fold reduction in fraudulent activity
- Eliminated in-game auction house and virtual currency abuse, saving the company millions of dollars
- Protection against account takeover
- Providing a safe and seamless gaming experience for genuine customers

Overview

The client is one of the world's largest sports video gaming companies that provides immersive, life-like gaming experience to its global user base. The company is known for its realism in the games and bringing the offline sports to life in their virtual avatars. It allows gamers to buy player personas and other merchandise using the virtual game currency, which can either be paid for in real currency or accumulated over a period of time.

The Business Problem

The global reach and scale of operations along with the associated financial gains made the company an attractive target for fraudsters. Fraudsters employed automated scripts to trigger thousands of matches automatically that completed hours of game sessions within a few seconds. Since gamers are rewarded with virtual currency on completion of a game session, the fraudsters accumulated loads of virtual currency, which they sold for real currency on third party sites and/or black market.

Apart from abusing the game servers, fraudsters used bots to create multiple fake accounts and cheat other players, act as fronts for illegitimate accounts, and level up the account profiles that could then be sold off to other gamers. They took over genuine user accounts to steal and monetize the virtual currency residing in these accounts. Fraudsters even abused the company's auction house to manipulate the in-game economy by taking over all assets/items and selling them at a premium or adding an influx of in-game currency, causing inflation. All these activities disrupted gaming experience for genuine users.

"We had very specific requirements as to how we wanted Arkose Labs to approach stopping the attacks. They are very flexible in tailoring attack mitigation techniques that align with our own unique security strategy."

— Manager • Fraud and Data Science

The Arkose Labs Solution

To thwart automated attacks and prevent fraudsters from abusing the gaming environment and game currency, the company deployed Arkose Labs solution. Within a short span of deploying the solution, the company saw fifteen-fold reduction in fraud activity and saved millions of dollars—all this without disrupting gaming experience for genuine users.

The key features of the bespoke solution that Arkose Labs deployed for the client are:

Deep Forensics

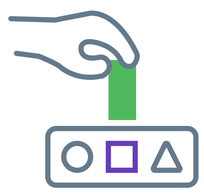
The Arkose Labs solution collates and analyzes digital intelligence including those from the originating devices, networks, and locations to gain insights into user profiles.

Continuous Intelligence

Combining these insights with behavioral analytics, the underlying intent of the user and associated risk are ascertained.

Enforcement Challenges

The Arkose Labs solution presents enforcement challenges to filter out bots and organized sweatshops from genuine users, which protects the company from malicious automated attacks. The insights from the Telemetry data combined with the risk assessment of the user, enforces stepped-up challenges for users with higher associated risk. While genuine users—98.6%— can easily clear these challenges, fraudsters must spend more time and resources.



On-brand

The enforcement challenges are custom-created using elements from within the games to blend with the overall game experience that minimize disruption and ensure seamless gaming experience.

The data from user sessions is fed back into the Telemetry which provides analysts with the required insights to adapt to the evolving attack types and future-proof their fraud prevention approach.

The multi-level, unified approach enables the client to effectively reduce automated attacks and provide a safe gaming environment to users around the globe, without compromising on their gaming experience.

Long-term Success

Fraud and risk landscape is rapidly evolving with new attack methods emerging everyday, making it hard for businesses to balance risk management with customer experience.As businesses focus deploy tools to stop attacks, fraudsters find ways to bypass those defences.

Arkose Labs believes that combating the growing online fraud epidemic requires a solution rooted in prevention and stopping of abusive attacks at the point of entry without disrupting user experience. Making the attacks more difficult and costly disrupts their economic incentive and breaks their business model. To clear the adaptive stepped-up enforcement challenges at scale, fraudsters must spend more time and invest in additional resources and machine learning. This continual increase in costs, renders the attacks economically non-viable. This results in a longer term solution and stops the cat and mouse game that fraudsters play with businesses.

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Schedule Demo

demo@arkoselabs.com
(800) 604-3319
arkoselabs.com