Arkose Labs

Travel Site Protects Business Critical Loyalty Points with Arkose Labs

CASE STUDY

Customer:

A major travel booking platform

⚠ Business Problem

- ATO attacks targeting customer accounts
- Fraudsters stealing customer loyalty points
- Customer acquisition and retention severely impaired

Solution

- Arkose Labs deployed on customer login flow
- Platform monitored traffic for signs of suspicious behavior
- Malicious bot traffic served anti-automation challenges

Results

- Attacks almost immediately stopped
- No impact to good user login flow
- Increased operational efficiencies

Overview

The client is one of the world's largest online platforms for booking travel accommodations. The company connects travelers with hotels, B&B's, and other lodging options in more than 80 countries around the world. As one of the largest travel platforms in the world, it sees a high amount of digital traffic on a daily basis.

The Business Problem

The platform is highly popular due to its great customer experience. One aspect of that is a robust loyalty points reward program. Consumers flock to the site to book travel and lodging in order to take advantage of rewards programs.

This also, however, caught the eye of fraudsters. The platform was dealing with a large amount of account takeover attacks, as fraudsters used bots to commit credential stuffing at scale in order to compromise user accounts. Once they got in, they would look to steal any accrued loyalty points that the user had attained. They can then use these points to buy hotel rooms, airfare, car rentals, and cruises for personal use, but more often they do it to then resell on a third-party platform.

In the highly competitive travel space, loyalty point programs are a key differentiator for businesses. Consumers often choose which platform they will do businesses with based on the strengths of the loyalty and rewards programs. If these programs are compromised, it inhibits the business's ability to attract and retain new customers.

These attacks were also severely hindering the experience for good users and resulting in a high amount of complaints being made to call centers, and well as damage to their brand reputation.

The Arkose Labs Solution

The company sought Arkose Labs after its previous fraud prevention vendor failed to effectively stop these attacks. The Arkose Labs platform was deployed on all login flows to monitor traffic and stop malicious actors.

Arkose Labs monitors all traffic for known signals of abuse, using behavioral fingerprints, velocity, and rate monitoring, and a proprietary user IP database. The solution embeds an Arkose Labs token into the web application or mobile SDK, and each request dynamically verifies that the token has passed from the client to the server.

Known malicious bot traffic is served with a dynamic enforcement challenge; these are 3D visual puzzles generated in real-time. They are designed against the grain of machine vision technology, meaning they cannot be solved by bots. The platform can also detect and stop organized human fraud attacks.

A 24/7 SOC is also on hand to work with each customer and respond to a spike in attacks if needed.

Results

After using the Arkose Labs platform, the company saw nearly all of the ATO attacks stopped almost immediately. Furthermore, this was done with no impact on good user sign-in flow, and the customer experience was drastically improved. Calls to contact centers were also drastically reduced, leading to operational efficiencies.

The Arkose Labs Advantage

Advanced Risk Classification

The Arkose Labs solution collects and analyzes digital intelligence, including data from the originating devices, networks, and locations to gain insights into user intent.

Real Time Challenges

Suspicious traffic is presented with step-up enforcement challenges. These are 3D images presented in real-time and are designed specifically to foil machine vision technology. The challenges are continually being updated and new ones are regularly created.

Privacy Focused

Arkose Lab technology achieves unparalleled accuracy without compromising data protection compliance.

Continuous Intelligence

Once combined with behavioral analytics, these insights help determine the underlying intent of the user, and the associated risk level is ascribed.

Seamless Customer Experience

Good users are never blocked, which eliminates the false positives that hinder customer experience and drain revenue.

Quick Implementation

New customers will see results within days, not weeks or months.

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication", the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput.

Schedule Demo

demo@arkoselabs.com
arkoselabs.com