Arkose Labs

Travel Site Eliminates Bots, Restores Business-Critical Booking Metric With Arkose Labs

CASE STUDY

Customer: Major Travel Booking Site

⚠ Business Problem

- The site was getting millions of bad bots per day scraping information
- This traffic was affected the site's contracted "look to book" ratio
- Dealing with massive daily bot traffic also put pressure on IT infrastructure

Solution

- Arkose Labs deployed to detect automated scraping activity
- Bots were served anti-automation enforcement challenges in real-time
- Good users faced no negative impact to their experience

Results

- Malicious bot traffic reduced by more than 99%
- Look to book ratio increased from 1% to over 6%
- Strain on cloud server usage greatly reduced

Overview

The client operates one of the world's foremost search engines for travel and booking, for both consumer as well as business travel. The site and its mobile app can be used to book hotels and airfare, along with car rentals, cruises, and more. With more than $10 billion in annual revenue, it is one of the largest travel booking sites in the world.

The Business Problem

For the world's foremost search engines for travel and booking, the "look-to-book" ratio is one of their key performance indicators. This critical travel industry metric shows the percentage of people who visit a travel website or mobile app compared to those who actually make a purchase.

The company is contractually bound with many of its providers within the airline and hospitality industry to maintain a certain ratio. However, when millions of bots set out to scrape information off their site, it damaged their ratio, as well as greatly strained their infrastructure. Since so many bots were coming to the site to scrape data and not purchase anything, the ratio hovered around 1%, which was lower than many of their contracts called for.

Furthermore, the site was facing a great strain on its servers due to the massive amount of bot traffic coming to it on a daily basis. This means there was far more usage than what would normally be anticipated on its cloud servers and created efficiency issues with its IT infrastructure.

The Arkose Labs Solution

The Arkose Labs Fraud & Abuse Platform was implemented on new user registration and login flows, as well as the company's search API, which bots were directly targeting. Arkose Labs detected this automated traffic coming to the site and served it with a proprietary enforcement challenge designed against automation.

These proprietary, interactive challenges are rendered in 3D and served in real-time, with countless possible variations. They are designed and tested to ensure that all automated attacks fail, are resilient to being solved en masse by computer vision technology, along with being resilient to large-scale human-driven attacks. Nearly all of the bot traffic to the site was unable to even load the Arkose Labs challenge, thus preventing it from accessing the site in any way or creating fake new accounts.

Meanwhile, legitimate users were able to pass through and authenticate without any disruption, meaning the client could maintain its stellar reputation around customer experience and digital ease of use that it is known for.

Demonstrated Results

The company had been seeing 35 million malicious bots hit their site per day; after implementing Arkose Labs that number was reduced by more than 99%. This enabled the client to raise its look-to-book ratio from around 1 percent to more than 6 percent, a significant increase that pleased its providers.

The client also greatly reduced the strain on its cloud web hosting platform due to tens of millions of fewer bot sessions on its website. This improved operational efficiency and allowed it to save money on server costs.

Key Advantages

Adaptive Decisioning:

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

Continuous Intelligence:

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

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 regularly created.

Seamless Customer Experience:

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

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