Arkose Labs

# Arkose Labs Helps Social Networking Site Reduce Web Scraping

CASE STUDY

## Customer: Global Social Media Platform

### ⚠ Business Problem

- Large-scale scraping of public profiles
- Targeting information which is the platform's source of revenue
- Difficulty differentiating between good traffic and malcious users

### Solution

- Arkose Labs detected and stopped automated attacks
- Malicious traffic faced repeated enforcement challenges, preventing scraping at scale
- Good users faced no negative impact to their experience

### Results

- 19% uplift in good user throughput
- 22% reduction in scraping
- Overall better customer experience for good users

"We are seeing higher legitimate user engagement alongside lower scraping activity, which are the critical metrics for us."

## Overview

The client is a major social media platform with more than 600 million users and a prime destination for networking, sharing content and job postings, among other things. It is a well-known and trusted brand among its customer base, however that same popularity has made it a major target for fraudsters looking to steal information from the platform.

## The Business Problem

This large social networking site was facing a major issue where fraudsters would employ bots at scale in order to scrape information from the public profiles of real users. For fraudsters, this information could then be used for malicious reasons, such as to create synthetic identities or launch targeted phishing scams. The platform needed to ensure it was protecting its users from downstream abuse.

Additionally, user information is core to the business' commercial viability. Offering products to third parties based on access to user information is the source of revenue for the platform. Therefore, anyone disseminating this information for their own purposes was in fact depriving the networking site of potential revenue millions of dollars. That's why it was so important for the platform to protect itself from this large-scale scraping of public profiles.

They had to ensure that any solution would not impact the experience of good users. This meant that they needed a scraping solution that would not simply block any traffic that might appear suspicious, but rather a more nuanced approach. They needed to better differentiate between automated scraping and good users who represented future revenue-generating customers. This was critical in order to protect consumers from downstream abuse that was fueled by the information gathered on their platform from the mass scraping.

# The Arkose Labs Solution

The social network decided to deploy Arkose Labs on their website in order to detect automated programs carrying out scraping activity and prevent malicious activity. When Arkose Labs detects potentially suspicious behavior - for example if one session viewed multiple user profiles, without logging in as a recognized user - they were presented with an enforcement challenge. Proprietary, interactive challenges are made using 3D visuals rendered in real time, with countless possible variations. These are designed and tested to ensure that all automated attacks fail, are resilient to being solved en masse by computer vision technology, and are resilient to large-scale human-driven attacks. Incrementally complex challenges are presented to bad actors attempting to gain information from the public profiles, in order to sap their time and efficiency and erode the potential profitability of attacks.

Legitimate users who may see a challenge, however, were able to quickly and simply solve them with no negative implications for the overall user experience. By preventing bad actors from carrying out scraping at scale, this eliminated the ROI of these attacks and led to attackers abandoning their efforts against the platform.

# The Arkose Advantage

The social networking site recognized that the Arkose Labs solution had a number of advantages over other solutions. Only a small amount of good users ever see a challenge, which they only have to complete once if they do see it.

### Reduce False Positives:

Rather than outright blocking, Arkose Labs instead profiles and classifies traffic, and pushes authentication challenges to suspicious traffic.

### 100% SLA Guarantee:

Authentication puzzles generated by Arkose Labs could not be solved by automation, even using the most robust machine vision tools.

### Seamless customer Experience:

Since no users are ever blocked, customer experience is not adversely affected. Good users rarely see a challenge, and if they do, they only have to complete it once.

### Intent-based Analysys of Traffic:

In-band authentication did not disrupt the users' flow and improved good customer throughput.

# Demonstrated Results

- 19% uplift in good user throughput.
- 22% reduction in scraping.
- Vastly improved experience for good users.
- Greatly reduced instances of false positives.
- Millions of dollars of potential revenue protected.

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