Arkose Labs

# Cloud Computing Provider Kicks Out Crypto Miners With Arkose Labs

CASE STUDY

**Customer:**

A Major Cloud Computing Provider

**Industry:**

Enterprise software

### ⚠ Business Problem

- Fraudsters created new accounts to take advantage of free trial server time
- Fake accounts were abused for cryptocurrency mining and other high-compute tasks
- Company experienced frequent cluster failures due to high volume attacks

### Solution

- Arkose Labs platform deployed on the new account registration flow
- Automated attacks detected and stopped
- Human fraudsters stymied until they gave up attacking

### Results

- Detected and stopped both automated and human-driven attacks
- More than 95% of fake new account fraud was stopped
- Server cluster failures were completely eliminated

## Overview

The client is a premier cloud computing platform which allows teams of developers to engage in projects related to data engineering, data science, machine learning and more. The company counts among its customers some of the largest global organizations in industries spanning financial services, retail, media, travel, healthcare and energy.

## The Business Problem

The platform is highly popular and used by engineering teams at many of the world's largest and most complex organizations. Its high visibility also made it a magnet for fraudsters. Attackers would use both bots as well as human fraud farms to sign up for fake new accounts in order to abuse free trials meant to entice new customers.

Fraudsters would use accounts with this free trial time in order to engage in tasks that required a high level of compute power, most notably mining cryptocurrency. This increased strain on cloud servers caused the company to experience cluster failures on a daily basis. On days with extremely high attack rates, upwards of 60% of clusters would fail due to the strain. This also greatly increased internal costs and manpower, as the company's internal security teams would have to work overnight fighting off the attacks.

## The Arkose Labs Solution

In order to stop these attacks, the company engaged Arkose Labs to be used as a first line of defense on the new account sign up flow. Arkose Labs was able to almost immediately stop nearly all of the malicious bot traffic, which was emanating from Russia. The platform is able to identify even sophisticated bots that are meant to appear as human. They are then served with targeted friction that is designed specifically against automation.

Arkose Labs also helped the client stymie persistent human fraud traffic that would not give up so easily. As soon as the automated attacks stopped, the platform detected fraud farm activity from Indonesia, attacking nearly 24 hours per day. Arkose Labs continually served this traffic increasingly difficult or timed challenges designed to frustrate human fraudsters and make them give up. After the attacks from Indonesia gave up, fraud farm attacks started again from other locales, including Singapore and Portugal, all of which were subsequently detected and stopped as well.

The whole time, the Arkose Labs 24/7 SOC worked closely with the client to fine tune the platform appropriately to defend against shifting attacks, and provide actionable insights for long-term mitigation.

## Demonstrated Results

Overall, these types of attacks were reduced by more than 95% since Arkose Labs was implemented. Furthermore, the measures that were used did not provide any hindrance to new customers signing up and taking advantage of promotional offers.

The company soon stopped experiencing cluster failures and realized greater internal efficiencies due to not having to constantly fend off attacks.

## The Arkose Labs Advantage

### 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 the associated risk level is ascribed.

### Real-Time Challenges:

These are 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 Fast Company Fintech Features and Cyber Defense Magazine, 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
arkoselabs.com