Arkose Labs

Arkose Labs Helps File Storage Platform Protect Millions of Accounts

CASE STUDY

At a Glance

Customer: Global technology platform

Business Problem

- Large-scale account takeover attacks
- Legacy authentication solution unable to stop bad actors
- Fraud mitigation tactics disrupted customer experience

Solution

Arkose Labs provided unified risk decisioning and targeted step-up authentication to differentiate between good users, bots and fraudsters, which helped eliminate automated attacks and sap fraudsters' time and resources.

Results

- Eliminated account takeover attacks
- Stopped fraudulent new account registrations
- Improved user experience
- Slashed intervention for customers by 70%

"With Arkose Labs, account takeover went from being our number one problem to a low priority issue."

- Director of Engineering

Overview

A global technology giant, which provides cloud storage and workspace collaboration to over 600 million registered users across 180 countries, turned to Arkose Labs to eliminate fraud attacks while improving the user experience for good customers.

Individuals and businesses across the globe rely on the platform to share, store and collaborate on critical information. The online accounts provide users with a trusted repository for sensitive data and files. Therefore, protecting the integrity of these accounts is a key priority for the company. The size and success of the company, however, made it a top target for fraudsters looking to abuse the sign-up process and hack into genuine user accounts.

The Business Problem

The technology platform had been experiencing a barrage of account takeover attacks. Fraudsters were also abusing the sign-up process for account enumeration--whereby attackers attempt to verify whether or not a user account exists. The company needed to increase defense against fraudsters attacking their platform, but without blocking good users.

The legacy solution was no longer fit for purpose as it was being circumvented at scale by bad actors using automated tools and cost-effective solvers. It offered no protection against human-driven attacks, but good customers experienced high intervention rates and were frequently being locked out of their own accounts. Authentication challenges were time-consuming and had low completion rates for legitimate humans. As a result, the company was inundated with support tickets from customers.

The company needed to better protect its user accounts, while dramatically enhancing customer experience.

The Arkose Labs Solution

Arkose Labs' solution was deployed on the technology platform to provide an intelligent mix of risk decisioning and step-up authentication. The risk engine, Arkose Enforce, analyzed real-time signals and behavior patterns in order to inform Arkose Detect, a step-up authentication mechanism, on whether a challenge was required. Depending on the risk profile, the solution adapted the nature and complexity of the challenges.

This targeted friction could withstand evolving attack patterns and deterred fraudsters from targeting the platform in the long-term. Enforcement challenges used the latest innovations in machine vision to ensure resilience to being solved en masse through automation, thus diminishing the profitability of attacks and undermining fraudsters' incentive.

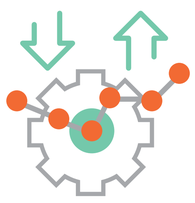
Only a small minority of true customers saw challenges, but whenever a challenge was presented to a good user they were fun and simple to complete. The company was able to reduce out-of-band authentication, which saved money and relieved the burden on the legitimate customers to prove they are legitimate.

"Our first line of defense against organized fraud is the Arkose Labs solution. We are delighted by the customization options and the high levels of service and attention we receive from the Arkose Labs team."

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

Dynamic Risk Engine:

Triage traffic using real-time intelligence and behavioral patterns to uncover the underlying intent of the user.



Intelligent Friction:

Target high-risk traffic with enforcement challenges, which accurately distinguish between authentic users, malicious humans and bots.

Adaptive Challenges:

Unique enforcement puzzles are designed and tested using the latest machine vision technology to ensure resilience to solvers and automated attacks.

Bespoke and Brand-integrated:

Inline authentication using the company's brand elements provides the most seamless user experience for good customers.

Demonstrated Results

Account takeover has gone from a top concern to a non-issue, freeing up team members to work on other efforts. There has been a 70% drop in intervention rates for customers logging into their accounts, resulting in improved throughput rates of good users. This has reduced the burden on in-house teams, slashed operational costs and improved customer satisfaction levels.

The combination of risk profiling and targeted authentication challenges effectively deters criminals, as they must now expend more time and resources to attack at scale. This makes attacks economically non-viable and provides the company with long-term protection against evolving fraud.

Arkose Labs bankrupts the business model of fraud. Its patented platform combines Arkose Detect, a sophisticated risk engine, with Arkose Enforce, which uses targeted step-up challenges to wear fraudsters down and diminish their ROI. The world's largest brands trust Arkose Labs to protect their customer journey while delivering an unrivaled user experience.

Schedule Demo

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