Arkose Labs

Dropbox protects millions of accounts using the Arkose Labs platform.

CASE STUDY

Dropbox

Business Problem

- Targeted by account takeover attacks
- Sign-up process abused for account enumeration
- User experience disrupted by existing step-up authentication

Solution

- The Arkose Labs platform provided unified risk decisioning to differentiate between good users, bots and fraudsters
- This solution was deployed alongside targeted step-up authentication to eliminate automated attacks and sap fraudsters' time and resources.

Results

- Greater resilience to account takeover attacks
- Intervention rates for customers slashed by 70%
- Stopped abuse of new account registrations

Overview

Over 600 million registered users across 180 countries--both individuals and businesses--rely on Dropbox to share, store and collaborate. With Dropbox accounts being used as a trusted repository for critical data and files, 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 users' accounts.

The Business Problem

Dropbox needed a solution that could act as its first line of defense against fraudsters attempting to perform account takeover and abuse the signup process for account enumeration.

Its legacy spam and abuse technology solution provided too much friction for customers, causing disruption to the user experience while at the same time not effectively stopping fraud attacks. Although more robust, out-of-band measures were also in place to prevent fraud, these as well were disrupting the login process for good users.

Dropbox needed a fresh approach to protecting users' accounts and turned to Arkose Labs for help. It needed to strike an optimal balance between seamless user experience, while stamping out fraud and abuse.

"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."

- Priya Bonthu, Engineering Leader

The Arkose Labs Solution

Arkose Labs provided Dropbox with powerful protection on its website, while enhancing the user experience for both new and returning customers. The Arkose Labs Fraud and Abuse Prevention Platform provided an intelligent mix of risk decisioning and step-up authentication to accurately identify malicious traffic from genuine users.

Arkose Labs provided Dropbox with powerful protection on its website, while enhancing the user experience for both new and returning customers. The Arkose Labs Fraud and Abuse Prevention Platform provided an intelligent mix of risk decisioning and step-up authentication to accurately identify malicious traffic from genuine users. The risk engine, Arkose Detect, analyzed real-time signals and behavior patterns to inform Arkose Enforce, 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 challenge presented to the user.

This combination provided targeted and informed friction, which was resilient to evolving attack patterns and deterred fraudsters from targeting Dropbox in the long-term. The 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.

Instead of presenting challenges to a significant proportion of customer traffic, Arkose Labs presented them only to a small group of good users. Simple, visual puzzles were easy for true customers to complete and prove their legitimacy, when necessary. This reduced reliance on out-of-band authentication, which was a burden for legitimate customers.

Key Features of Arkose Labs Fraud and Abuse Prevention Platform

Dynamic Risk Engine: Triage traffic using real-time analysis 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.

Interactive Challenges: Unique enforcement challenges 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 Dropbox brand elements to provide seamless user experience for good customers.

Demonstrated Results

The combination of risk profiling and targeted authentication challenges deters bad actors from attacking Dropbox, as they must now expend more time and resources to attack at scale. This makes attacks economically non-viable and provides Dropbox with long-term protection against fraud.

A 70% drop in intervention rates for customers logging into their accounts has resulted in improved good throughput. This has reduced the burden on in-house teams as well as the operational costs of dealing with customer service tickets.

"Arkose Labs has proved to be a long-term deterrent to fraudsters attacking our website, allowing us to stamp out account takeover attacks and keep our customers protected."

- Priya Bonthu, Engineering Leader

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