Arkose Labs

E-signature Company Protects Valuable Digital Documents with Arkose Labs

CASE STUDY

Customer:

A Prominent e-Signature and Document Management Firm

⚠ Business Problem

- Credential stuffing attacks targeted user accounts
- Legacy solution struggled against volumetric attacks
- User experience was being disrupted by continual bot attacks

Solution

- Arkose Labs platform deployed to detect and stop malicious traffic
- Real-time enforcement challenges cause all automated attacks to fail
- User-friendly authentication reduced friction for customers

Results

- Immediate drastic decrease in attacks
- No impact to good user throughput
- Millions of user accounts protected

Overview

The client is one of the world's leading e-signature and document workflow services. It serves hundreds of millions of users around the globe, who trust and rely on it to provide a safe and secure platform for signing and storing important digital documents. Its product suite spans core capabilities such as digital signature and online fax as well as fully customizable document workflow solutions for businesses.

The Business Problem

Documents are vital to many of life's important tasks -- such as opening a financial account, signing a lease, taking out a loan, applying for college and more. Digitally signing and storing these documents is much more efficient for businesses and consumers than storing physical paperwork.

The client is a global provider in digital signatures and documentation and is trusted by consumers and businesses worldwide. However, since these documents contain extremely sensitive and potentially valuable personal information, such as social security numbers and financial account information, they are a target for fraudsters. As such, the client was seeing credential stuffing attacks on its login flow, as attackers sought to compromise user accounts and gain access to the sensitive and potentially valuable information contained therein.

The fraud prevention solution in place at the time was ineffective in stopping these account takeover attacks at scale. As machine vision technology has advanced, most fraudsters are able to purchase off-the-shelf bot programs for little money that can easily overcome many solutions. Furthermore, its detection engine was not robust enough to recognize and challenge all of the malicious IPs coming to the site.

The Arkose Labs Solution

The company sought a new fraud prevention and account security solution with more robust analytics and insights and the ability to stop volumetric attacks. It came across Arkose Labs since the platform was in use by its parent company, which recommended the platform as effective in providing long term deterrence against fraud attacks for its 700 million users..

The Arkose Labs Fraud and Abuse Platform combines real-time intelligence, rich analytics, and adaptive step-up challenges to progressively diminish the profitability of attacks while adapting to evolving attack patterns. Arkose Labs' risk detection combines rich data intelligence with powerful analytics to discern intent and behavior in real-time. The platform was able to detect and stop malicious traffic coming to the company's platform at a much greater degree than its previous solution.

Arkose Labs' customer success team also worked 24/7 with the client to offer actionable insights and tailored solutions customized to the unique threats that it faced.

Demonstrated Results

After implementing Arkose Labs, the company saw an almost immediate stop to the credential stuffing attacks that had been targeting their platform. Arkose Labs' robust detection engine was able to effectively recognize malicious traffic coming to the site and served it enforcement challenges that stopped attacks before they were able to hit the login point. Meanwhile, good users saw no impact or friction and enjoyed the same stellar digital user experience they had always enjoyed.

> After implementing Arkose Labs, we saw an immediate ROI. The credential stuffing attacks stopped, and they have been a great partner with us in fighting fraud."
>
> Engineering Manager

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.

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.

Continuous Intelligence:

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

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 "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