Arkose Labs

Arkose Labs Helps a Leading Digital Banking Platform Prevent a Myriad of Fraud

CASE STUDY

A Leading Digital Banking Platform

Business Problem

- Credential stuffing
- Automated account takeover attacks
- Abuse of convenient onboarding facility for fraudulent new account origination
- Payment fraud
- Fraudulent loan applications
- Phishing customer details

Solution

Arkose Labs solution filters out bots and organized sweatshop attacks on the company's digital banking platform by making the attacks non-viable through adaptive stepped-up Arkose Enforce challenges

Results

- Protection against account takeover
- Streamlined new account origination
- Prevention against payment fraud
- Prevention against fraudulent loan disbursal
- Safeguarding customer relationships by blocking phishing attempts

Overview

The company is a leading technology company that provides a comprehensive digital banking platform. This platform comprises technology solutions that enable financial institutions and their customers to securely communicate and transact – anytime, anywhere, using any device. It provides flexible deployment options for online banking, mobile banking, and voice banking to financial institutions. Through its group companies, the company helps financial institutions with hassle-free account onboarding for the mobile-first customers, and close loans faster.

The Business Problem

Although digital disruption and availability of innovative products are enabling financial institutions to quickly onboard new customers, disburse loans instantly, or upsell targeted products, they are also making a larger attack surface available to fraudsters.

The success of the company's platform faced a setback when fraudsters began using personally identifiable customer data and easily available tools to attack the platform and monetize their exploits. Fraudsters would abuse the convenient onboarding facility for fraudulent new account origination. They would resort to credential stuffing and impersonating genuine customers to attempt account takeover of accounts and abuse the platform to seek instant approval for fraudulent loans and credit cards. They even manipulated the platform's targeted messaging system to phish out customer details.

All these activities not only disrupted user experience for end users but also began damaging the company's relationships with its customers.

"We analyzed the problem internally and deployed fraud prevention solutions without much success. We then approached Arkose Labs and within a few days fraud rates dipped dramatically. Arkose Labs has helped us maintain customer relationships, so crucial in growing a business like ours."

—Lead • Fraud Prevention Team

© 2021 Arkose Labs. All rights reserved.

The Arkose Labs Solution

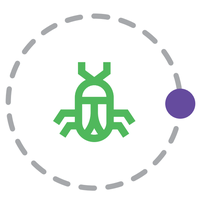
The company conducted an internal analysis to identify the pain areas and deployed ReCAPTCHA but the results did not change. They approached Arkose Labs for a resolution and within a short span of deploying the bespoke solution, there was a significant reduction in fraud without disrupting customer experience. The Arkose Labs solution helps the company monitor logins to protect against credential stuffing, account takeover, streamline new account origination, prevent payment fraud, prevent fraudulent loan disbursal, and most importantly safeguard customer relationships.

The Arkose Labs Fraud and Prevention Platform helps global brands fight fraud and online abuse by rendering the attack economics non-viable. It continually diminishes the returns from an attack by presenting adaptive step-up challenges that require fraudsters to spend more time and resources. For bot-driven automated, scripted, and/or human-driven attacks through click-farms and sweatshops, fraudsters must invest in machine learning and machine vision to clear these challenges at scale—a costly proposition which makes the attack non-profitable.

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

Device and Network Forensics

The Arkose Labs solution deduces specific intelligence for individual users by collating and analyzing digital intelligence including those from the originating devices, networks, and locations.



Historical Attack Pattern Intelligence

Unearth hidden patterns and correlate them with the attack patterns across use cases to demonstrate how attacks are orchestrated.

Continuous Intelligence

The solution combines the insights with behavioral analytics to accurately understand the underlying intent and the associated risks of the users to assign risk profiles to every user.

Adaptive Arkose Enforce Challenges

Insights from the Arkose Enforce data combined with the risk assessment of the user, enforces adaptive, stepped-up challenges for suspicious users. This helps filter out bots and organized sweatshops from genuine users and protects the client from malicious automated attacks. Genuine users face no difficulty clearing these challenges, while fraudsters must spend more time and resources.

Long-term Approach

The data from user sessions is fed back into the self-optimizing Arkose Detect which powers continual enhancements to Arkose Enforce and provides analysts with the required insights to adapt to the evolving attack types which future-proofs their fraud prevention approach.

A multi-tiered, long-term approach enables the company to effectively fight a number of automated attacks and provide a secure digital banking environment to their users, while ensuring a seamless user experience.

---

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

Schedule Demo

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.

© 2021 Arkose Labs. All rights reserved.