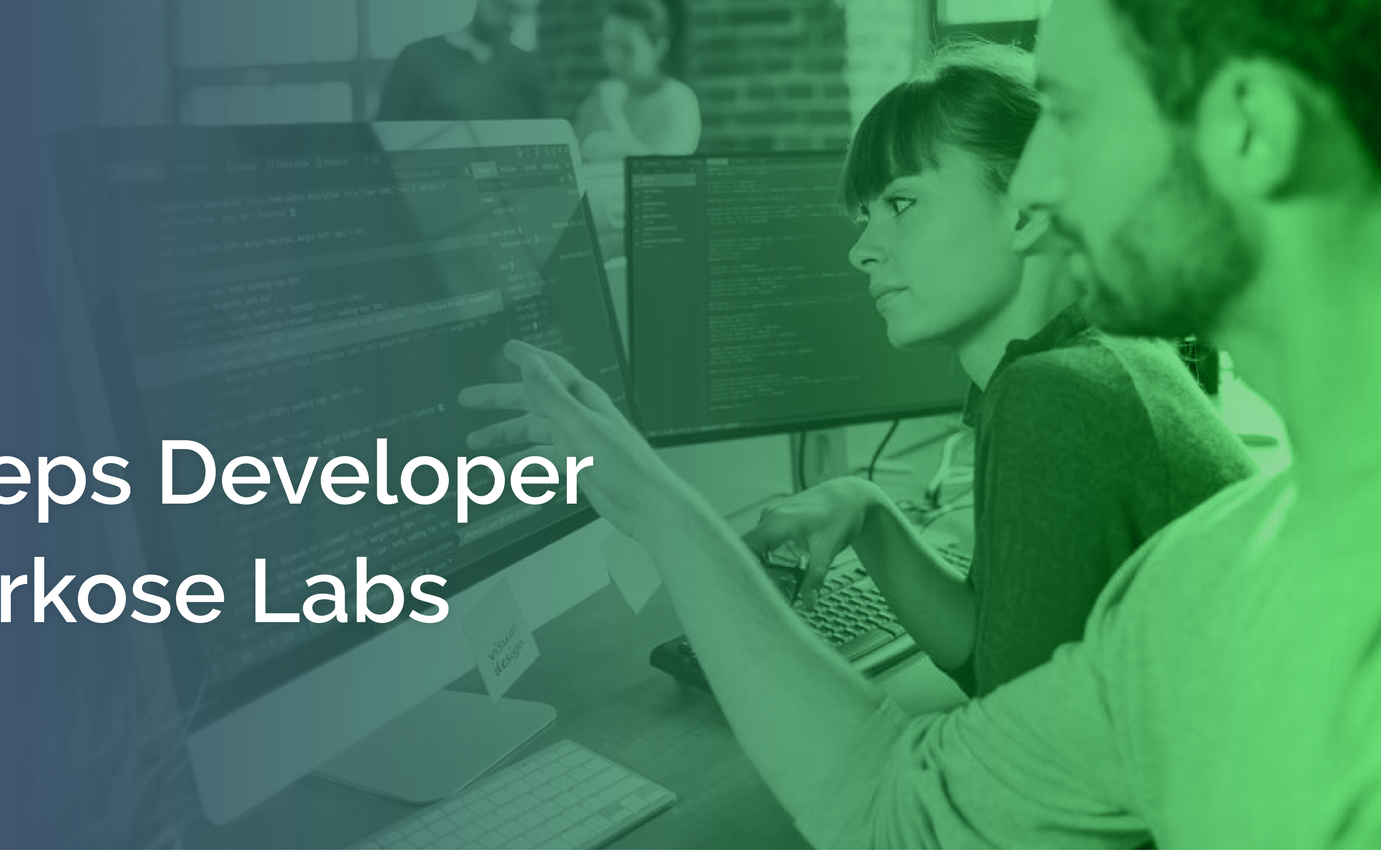
Arkose Labs



Technology Platform Keeps Developer Environment Safe with Arkose Labs

CASE STUDY

Customer: A Major Tech Platform

⚠ Business Problem

- Fraudsters taking advantage of free new account registrationt
- Protective measures taken to stop attacks caused customer friction
- Manual reviews led to internal inefficiencies and loss of revenue

Solution

- Arkose Labs deployed on New Account registration flow
- Arkose Labs monitored all traffic for signs of suspicious activity
- Detected and stopped even sophisticated attacks designed to hide identity

Results

- Fake new account attacks stopped
- Increased operation efficiency
- No impact to good user experience

Overview

The client is a major American technology and IT services company with more than 15,000 employees. The company has diversified offerings, providing software encompassing customer engagement, CRM, information management, location management, and more to its enterprise customers. It is one of the most respected business services companies in the world.

The Business Problem

As part of its commitment to innovation, the company allows developers to register for free to its sandbox environment so they can configure APIs for their particular business needs. However, fraudsters could potentially take advantage of this to create fake accounts and abuse the sandbox environment.

The company was using an incumbent identity solution, however, it was not happy with the solution's ability to detect the fraudulent new account signups in real-time. The solution was also unable to detect many of the current sophisticated tactics used by fraudsters.

To ward off potential fake new account attacks, the company required any new signups to reach out via email to create an account. This method, however, strained internal resources due to the sheer number of manual reviews that had to be performed. The increased internal labor hours to do this was inefficient for the company due to the low margins this particular product had for the company's overall business. Furthermore, it created too much friction for good users trying to sign up.

The Arkose Labs Solution

Looking for a more optimal solution, the firm contacted Arkose Labs. The company performed a technical test of the Arkose Labs product and found that its approach to long-term deterrence of fraud attacks was the best solution for the problem it was facing.

Arkose Labs monitors all traffic for known signals of abuse, using behavioral fingerprints, velocity, and rate monitoring, and a proprietary user IP database. The solution embeds an Arkose Labs token into the web application or mobile SDK, and each request dynamically verifies that the token has passed from the client to the server.

Known malicious bot traffic is served with a dynamic enforcement challenge; these are 3D visual puzzles generated in real-time. They are designed against the grain of machine vision technology, meaning they cannot be solved by bots. The platform also frustrates persistent human attacks to the point where they give up and attack other platforms. Furthermore, a 24/7 SOC is also on hand to work with each customer and respond to a spike in attacks if needed.

Ultimately, the company recognized that other solutions weren't going to be able to solve the at-scale attacks they were having on the signup flow.

Results

The vast majority of the fake new account attacks were stopped within a short amount of time of implementing the Arkose Labs platform. Just as importantly, the company did not have to devote internal resources to manually approving or rejecting new account sign-up requests. This not only saved vast amounts of time and created efficiencies but created long-term cost savings for the company.

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

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 are regularly created.

Seamless Customer Experience

Good users are never blocked, which eliminates the false positives that hinder customer experience and drain revenue.

> Arkose Labs has been a great partner in working with us to maintain a secure and user-friendly environment for our developer community.

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