Arkose Labs

Arkose Labs Enables Ecommerce Giant to Stop New Account Fraud

CASE STUDY

Customer: Global e-commerce platform

⚠ Business Problem

- The client struggled with bots and human sweatshops creating fake new accounts
- These accounts were used to commit numerous types of downstream abuse
- Efforts to quell fraud were degrading the user experience for good customers

Solution

- Arkose Labs was deployed at the new account creation and login stages
- Suspicious traffic was identified and served an anti-automation enforcement challenge
- Real-time data logging provided insights on traffic volume and attack patterns

Results

- 54% reduction in fake new accounts created
- Significant reduction in downstream abuse
- Data insights assisted the client in creating a holistic risk operations strategy.

Overview:

The client operates one of the world's largest e-commerce platforms and connects millions of buyers and sellers globally. As one of the largest digital platforms in the world, it is a big target for fraud. The continued success relies on protecting its massive user base from fraud, abuse and scams.

The Business Problem

The company was having an issue stopping fake new account creation. Bad actors would employ bots or teams of human fraudsters to create new accounts at scale, which could then be used to commit a wide range of downstream abuse including leaving fake reviews or fake ratings, selling fake items with no intention of shipping any product, and sending spam messages to other users. These accounts could then be activated time and again to continually commit fraud.

The company used an in-house fraud detection and prevention solution that proved to be largely ineffective in stopping these attacks. Further, the solution was catching good users in its net, leading to an often onerous authentication process and providing too much friction. Fraud was running rampant while good users were being frustrated.

Arkose Labs Solution

The client deployed the Arkose Labs Fraud and Abuse Platform to compare results against its homegrown solution. Arkose Labs was deployed on the new account creation flow in Europe, North American and Asia, and the client and Arkose Labs teams collaborated on identifying traffic patterns and continually tuned the platform to accurately identify attack types, and user behavior.

The platform was able to adapt to real-time signals and changing traffic patterns to determine the intent behind traffic to the client's site. Suspicious traffic was triaged into either trusted or potentially fraudulent. It was then served an enforcement challenge, which provide an innovative and user-centric method to slash malicious traffic. There is a deep bench of 3D puzzles, which are designed against the grain of machine vision technology to prevent bots being trained to solve them at scale. They are rendered in real-time using technology that allows for countless possible permutations and are backed by a SLA guarantee that they will protect businesses from automated attacks. Good users will rarely see the challenge but if they do it is easily solvable and they will be able to pass through without being challenged on further log-in attempts.

Real-time data logging provided the client insights on traffic volume and attack patterns. They were able to see deep analytical insights into user interactions with different challenge types and benefit from an intuitive dashboard that uses visualization and data stitching to deliver end-to-end insights across the customer journey. This unifies user data with real-time user behavior and metadata.

Furthermore, Arkose Labs challenges were white-labeled so the client's branding appears on them. This helped to optimize the customer experience and make solving the challenges -- should a good user encounter one -- feel like a seamless experience within the client's platform.

Demonstrated Results

After implementing Arkose Labs, the company immediately saw a **54%** reduction in fraudulent new accounts created as compared to the incumbent solution. The company also realized a significant reduction in downstream abuse and chargebacks because of the early detection of fraud attacks by Arkose Labs. In one specific case, the company was able to identify and stop a sweatshop attack originating from Bangladesh that it otherwise would not have detected prior to implementing Arkose Labs.

Additionally, the client was able to accurately identify peak times when fraud attacks occurred and allocate resources appropriately. Overall, real-time data insights provided by the Arkose Labs platform assisted the client in creating a wider, more robust holistic risk operations strategy

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.

Schedule Demo

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