

# Waste Fraudsters' Time, Not Yours

## Arkose Labs Fraud and Abuse Prevention Platform

Businesses across industries have seen a dramatic increase in fraud over the last 12 months. Why? With an abundance of stolen data and easy-to-use technology, fraudsters can launch bot attacks at scale for \$15 a day or less. Their model is to make as much money in as little time as possible, and it works.

Meanwhile, security & fraud teams are working tirelessly to detect fraud and challenge suspicious traffic without creating too much friction for good customers. With determination, fraudsters continuously come back with more sophisticated tactics. It's an endless game of keep-up that costs business resource time, customer trust, reputation, and more.

*Isn't it time fraudsters resources were drained instead of yours?*

## Arkose Labs Makes it Uneconomical to Attack You

The Arkose Labs platform cuts fraud off at the source by making cybercriminals expend massive effort to conduct their attacks. This erodes their ROI until the attack is no longer economically viable. This is a fundamental shift in fraud prevention; one that plays that long-game with you against fraudsters.

### Protection Across the B2C Digital Perimeter



#### ACCOUNT REGISTRATION

Fake Account Registrations | Bonus Abuse | Credential Testing

- Understand true intent of new users
- Detect bulk fake account openings
- Reduce downstream fraud or banning
- Long-term account protection



#### ACCOUNT PROTECTION

Account Takeover | Credential Stuffing | Loyalty Point Theft | Payment Fraud

- Protect user accounts in real time
- Slash MFA and authentication tokens
- Eliminate large-scale attacks
- Improve user login experience



#### BOTS AND ABUSE

Spam | Fake Listings & Reviews | API Abuse | Web Scraping | Inventory Hoarding | In-Game Abuse and RMT

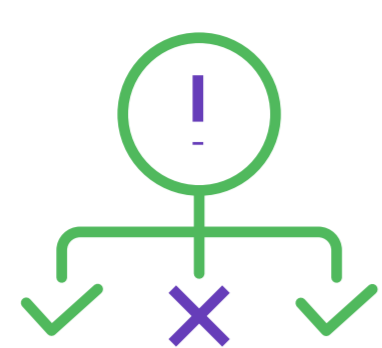
- Protect the integrity of platforms
- Eradicate malicious bot traffic
- Protect users from scams

## Arkose Labs Fraud & Abuse Prevention Platform

Combining a dynamic risk engine with adaptive step-up authentication, the Arkose Labs platform does the heavy lifting to distinguish good vs. bad intent and expertly challenge only suspicious traffic in real-time.

Challenges are tailored to the signature tactics of large-scale bots, trained bots, and human fraud farms, while eliminating friction for good users with increased confidence. The result is a secure and seamless digital experience for good users, while stamping out abuse in all its forms on your website and apps.

# The Arkose Labs Approach



## Classify Risk

### Arkose Detect

Sophisticated decision engine classifies traffic into risk categories, segmenting suspicious traffic for tailored friction with superior confidence.



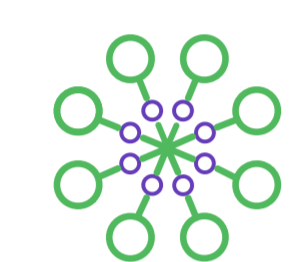
Deep device and network forensics



Behavior analytics



Location assessment



Embedded machine learning



## Challenge & Interact

### Arkose Enforce

Adaptive challenges present friction to high-risk traffic in real-time, eroding fraudsters' ROI while determining true intent.



Anti-automation challenges



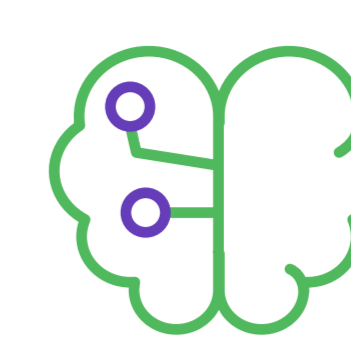
Human fraud challenges



Accessibility & language support



Interaction Feedback Loop



## Analyze and Learn

### Arkose Global Network

Data from our global network feeds anonymized threat intelligence back into the platform, continuously improving with evolving threats.



Database of known attack telltales



Visualizations of network insights



Anomaly detection



Historic attack pattern calibration



Arkose Labs offers an industry-first SLA guarantee to protect customers from automated attacks.



Commercial assurance on the efficacy of the platform



Backed by a 24/7 SOC to assist with emerging threats

## Global Brands Winning Against Fraudsters



33% improvement in customer throughput vs SMS



Slashed intervention rates for good customers by 70%



Automated new account creation eliminated entirely



*"The difference between our past solution and Arkose Labs is night and day for us. Previous solutions created a bad user experience. Arkose Labs solves our problem with no added friction, and makes it fun for our users." - Engineering Director, Roblox*



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.