Arkose Labs | SOLUTION BRIEF

Arkose Labs' Fraud Deterrence & Account Security 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 opening
- 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 Listing & 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

Stop Bots & Fraudsters, Not Good Users

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.

Arkose Labs Fraud Deterrence Platform

Arkose Labs delivers long-term account protection and fraud deterrence by undermining the economic drivers behind attacks. Our AI-powered platform detects persistent bots and coordinated human attacks on the most targeted user touchpoints on websites and apps. Invisible risk assessments allow good users to pass through seamlessly. High-risk traffic is triaged for active attack response using innovative enforcement challenges that deter future attempts, while delivering a more secure experience for genuine customers.

Arkose Protect™ *Full Spectrum Detection & Response*

Arkose Detect™ *Defense-in-Depth Detection*

Real-Time Detection

Device, network, and behavioral assessment

ML Decision Engine

Rules engine powered by global intelligence

Insights & Data Sharing

Transparent risk scoring with deep data sharing

Dynamic Attack Response

User-centric authentication & attack remediation

Arkose Detect: Real-time Risk Classification

Arkose Detect collects real-time intelligence to unearth fraudulent behavioral patterns across devices, networks, and third-party risk engines. It accurately uncovers the underlying intent of the user, which helps you confidently choose the most appropriate response strategy.

Device ID & reputation

Deep device forensics is used to fingerprint devices based on its characteristics and integrity over time. Works for desktop, mobile, smart TVs, and gaming consoles.

Network & IP assessment

Arkose Labs combines a proprietary IP scoring system with 3rd party reputation lists to monitor for abnormalities such as spoofing location or using cheap IP addresses.

User Behavioral Analysis

Behavioral biometrics such as keystroke, gyroscope, and page familiarity are used to distinguish good user behavior automation and bad human behavior.

Customer Data Exchange

Our flexible APIs can ingest data from proprietary or third-party risk engines to improve risk assessment accuracy and inform the usage of Arkose Labs' enforcement challenge.

Never Choose Between Strong Security & User Experience

The combination of risk decisioning and targeted enforcement allows platforms to be more aggressive against persistent attacks without fear of impacting good users. In the event of a false positive, Arkose Labs' user-centric secondary screening diminishes the risk of good users being blocked or impacting conversion rates.

- High-risk traffic is challenged, never blocked
- Targeted enforcement increases customer throughput by 20%+
- 99% of flagged good users solve a challenge on the 1st try
- Challenge interaction data trains the decision engine
- Improve user experience by reducing reliance on MFA

ML Decisioning & Data Sharing

The Arkose Labs platform is centered around an AI-driven decision engine that processes real-time signals with our deep historical intelligence. With 150+ global rules out of the box, the Arkose Labs platform detects signs of fraud on day 1 that others miss. Risk classifications are backed by deep sharing to make threat intelligence more actionable.

Machine learning framework

Embedded machine learning assesses anomalies from real-time signals, historical attack patterns, and attacks across the Arkose Labs Global Network of customers. Our AI-driven platform evolves models in real-time to rapidly adapt to evolving attacks.

Attack pattern correlation

Arkose Labs takes a storytelling approach to fraud. Rules and patterning correlates fraud tell-tale signals, velocity and distance, and historical customer behavior to validate whether or not a user's story checks out.

Response orchestration

Combining real-time insights with the risk profile of the user, our dynamic defense determines the appropriate step-up challenges for the risk profile. The orchestration hub is supported by a behind-the-scenes team monitoring traffic flow and attack patterns to adjust telltales and enforcement challenges accordingly.

Open Data Sharing

Unlike black-box solutions, Arkose Labs provides 70+ raw risk signals for better visibility behind each risk score. All risk signals collected by Arkose Labs can be ingested into existing models to improve decision accuracy early in the user journey, while providing better insight downstream.

Arkose Protect: Detection + Attack Response

Arkose Protect provides full-spectrum detection plus the power of user-centric challenge-response to stop attacks before they cause damage. When traffic is flagged as suspicious, Arkose Protect provides secondary screening and targeted attack response that breaks the economics of bot and human-driven attacks. Challenges collect user interaction data to further validate the user's intention and deliver truth data back to the decision engine.

Bot Defense

Suspected bots are presented with a deep bench of challenges that machines have no idea how to solve. No off-the-shelf technology can be used to solve our challenges, forcing fraudsters to continuously build AI, wasting time and resources.

Human Challenges

The Arkose Labs platform presents time-absorbing challenges when attackers use human labor to circumvent anti-bot technology.These challenges deliberately waste the time and resources of the fraud farm, making it unprofitable.

Risk Score & Real Time Logging

An open API platform enables customers to ingest honest and transparent data directly from Arkose Labs. With our real time logging API, customers can access insights from all sessions to enhance risk models.

Attack SLA & Warranty

Arkose Labs is so effective against even the most persistent bots, we stand by our customers with a contractually guaranteed attack SLA and an industry-first credential stuffing warranty.

Arkose Global Network

Arkose Labs takes a consortium approach to fraud, leveraging anonymized threat intelligence from over 4.1B IP addresses across a vast global network of customers each year. From day 1, Arkose Labs customers benefit from a database of over 4,000 tell-tale fraud patterns.

The Arkose Advantage

Guaranteed Efficacy
Powerful protection backed by commercial assurance and industry-first limited warranty

Privacy Friendly
Arkose Labs technology achieves unparalleled accuracy without compromising data protection compliance

Minimum Friction
Unified workflow brings together the detection and the proprietary challenge. The lower the risk is, the easier is the challenge

Early Detection
Eliminate losses, reduce costs, and streamline efforts by preventing attacks before they advance in your ecosystem

Managed Services
Arkose Labs empowers your teams by working as a true partner in fighting fraud and delivering insights specific to your business

Results Fast
New customers will see results within days, not weeks or months.

Fintech Neobank Beats ATOs

One of the world's most prominent fintech firms was targeted by bots executing credential stuffing attacks at scale. Successful attacks lead to the draining of customer funds and poor user experience.

Impact:

- Appeared less trustworthy to customers and damaged overall relationships
- High repayment costs as a result of ATOs

Results:

- 75% reduction in ATO attempts
- Slashed compromised account costs previously hitting $100,000 per week
- Resources saved from reduction in resetting credentials on compromised accounts

Dropbox Protects Millions of Accounts With Arkose Labs

Dropbox utilized the Arkose Labs Platform to stop fraudsters looking to abuse the sign-up process and hack into genuine users' accounts.

Impact:

- Sign-up process abused for account enumeration
- Existing solution created too much friction for users

Results:

- Greater resilience to account takeover attacks
- Intervention rates for customers slashed by 70%

Microsoft Outlook.com Tackles Fraud & Abuse

Outlook.com was the target of fraudsters looking to create fake accounts at scale to then disseminate spam and malicious content.

Impact:

- SMS tokens were expensive and circumvented by attackers
- Customer throughput was also impacted by SMS

Results:

- 98% reduction in fraud and abuse
- 33% increase in good user throughput

Arkose Labs bankrupts the business model of fraud. Recognized by Fast Company Fintech Features and Cyber Defense Magazine, 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.

Email:
demo@arkoselabs.com

Schedule Demo