Arkose Labs | SOLUTION BRIEF

Arkose Labs for Financial Services and Fintech

With the further digitalization of the financial industry, fraud prevention and account security has become a top concern for companies in this sector. The industry of fraud functions on spending the least amount of time and resources on an attack in order to achieve the most monetary gain. This makes finance and fintech companies an attractive target for fraudsters due to the potential of stealing large sums of money. With financial companies having to adapt to an increasingly digital world and fraudsters constantly creating new advanced attack strategies, cybercrime is no longer an issue companies can ignore.

When it comes to their finances, customers look for banks and services they can trust to keep their accounts secure. Customers of financial companies want a seamless user experience without taking risks with their financial security. Businesses need to find the most effective security measures that weed out bad traffic early and maintain a positive user experience without high authentication costs.

Arkose Labs Bankrupts the Business of Fraud

As long as there is profit to be made, fraudsters will continue to attack. Arkose Labs bankrupts the business of fraud by sabotaging attackers' ROI and making it uneconomical to attack companies in our network. This is a fundamental shift from fraud prevention to fraud deterrence.

Global finance companies trust Arkose Labs to detect and deter attacks at user authentication touchpoints where account takeovers, payment fraud, credential stuffing, and fake account creation attacks originate. By rooting out fraud early, companies are able to strengthen relationships with customers by offering an increasingly secure financial platform without sacrificing a positive user experience.

Protection for the Most Targeted User Touchpoints

Account Takeovers
Protect user accounts against credential stuffing and account takeovers, which puts users' critical financial accounts at risk.

Advanced Persistent Bots
Most robust protection against advanced bots that bypass traditional bot defenses to blend in with user traffic.

Micro-deposits & Payment Fraud
Protect any user action within web and mobile applications, for example adding linked accounts that are abused for micro-deposit fraud.

Bots and API Abuse
Advanced bots are consistently bypassing traditional bot defenses, attempting to blend in with traffic at logins, account sign-ups or targeting APIs directly.

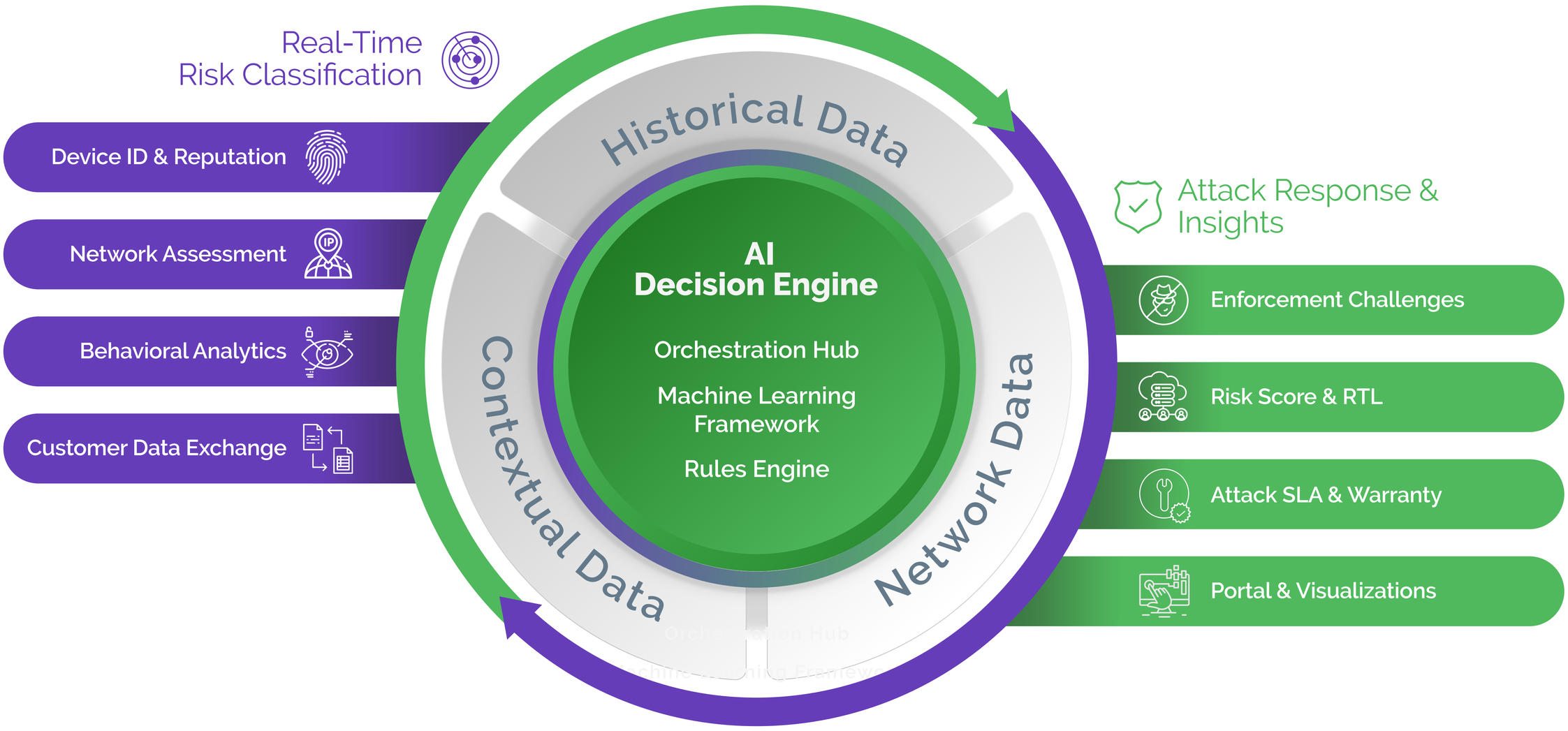
Application Fraud
Stop fraudsters leveraging stolen and synthetic credentials to set up fake new accounts for fraudulent purposes.

Bonus Abuse
Secure user promotions from abuse by fake users, such as a cash bonus for signing up to a new card or a fintech platform.

API Abuse
Stop attacks on APIs from advanced bots emulating clients and impersonating legitimate users.

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 defeats 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 Decision Engine: Big data & advanced analytics

The Arkose Labs platform is centered around an AI-driven decision engine that processes real-time signals with our deep historical intelligence to orchestrate a targeted attack response. From real-time and challenge interaction data, ensuring that genuine users are able to pass seamlessly whilst detecting evolving attack techniques.

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.

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.

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 informs the appropriate attack response.

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.

Arkose Enforce: Attack response & deterrence

When traffic is flagged as suspicious, Arkose Enforce 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 know 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

Arkose Enforce 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.

Solving the False Positive vs False Negative Conundrum

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	Invisible screening means customers rarely see challenges	Flagged good users easily solve challenges on the first try	Challenge interaction data trains the decision engine	Improve user experience by reducing reliance on MFA

The Arkose Advantage

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

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

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

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

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

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

Arkose in Action

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

Global Bank Protects Logins and Stops Application Fraud

The client is one of the largest global banks, with millions of retail customers around the world and heavily targeted by loan application fraud and ATO attacks.

Impact:

- Threatened customer account security due to financial and identity theft
- Mass automated attacks became mass revenue loss with having to repay stolen customer funds

Results:

- Proven superiority in stopping automated attacks
- Improved user experience versus reCAPTCHA approach

Blackhawk Network Puts an End to Carding

Blackhawk Network is a rapidly growing payment company with innovative solutions that enable gift card use in the digital realm. It is trusted by retailers and consumers alike.

Impact:

- Fraudsters would test stolen gift cards and prepaid cards to drain the remaining balances leaving the company to repay the victims of stolen cards.
- Other bot and human-driven attacks on their website caused a poor user experience.

Results:

- 98% reduction in bot attacks
- 60% reduction in human-driven fraud

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

© 2021 Arkose Labs. All rights reserved.