Arkose Labs | SOLUTION BRIEF

Arkose Labs for Retail

Protect Accounts and Consumer Trust with Early Fraud Detection

As the digital buying experience becomes more seamless everyday, it's getting hard to tell a good customer from a skilled fraudster. Advancements in technology have enabled fraudsters to mimic good user behavior and blend into the traffic, exploiting every customer touchpoint and convenience to orchestrate attacks further upstream than ever before.

Large scale attacks and rampant abuse disrupt user experience and most importantly the trust of consumers. Trust is the currency that powers commerce. It takes multiple interactions to build trust, and a breach of this trust can impact repeat purchases and overall brand loyalty. As fraudsters continually upgrade their techniques through compromised and fake accounts, protecting buyers has become more important than simply protecting transactions.

Throughout your entire digital experience—mobile, desktop, or native mobile apps—you want to create a secure environment for customers to transact from the very beginning.

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 you. This is a fundamental shift from fraud prevention to fraud deterrence.

Global retailers trust Arkose Labs to detect and deter attacks at user authentication touchpoints where account takeover, fake account creation, bonus abuse, inventory hoarding, and scraping originate. By rooting out fraud early in the customer life cycle, you'll reduce stress on the payment flow and have greater confidence it's a real customer at checkout.

Protection for the Most Targeted User Touchpoints

Account Takeovers
Protect user accounts against credential stuffing anaccount takeovers, which leads to downstream abuse including changing user credentials, fraudulent purchases, and payment fraud.

Denial of Inventory
Prevent inventory hoarding from automated bots which add items to shopping carts to prevent legitimate purchases, in order to make money or disrupt a competitor.

New Account Fraud
Streamline the account sign-up process and prevent fraudsters from using stolen or fake user credentials to abuse promos and disseminate spam.

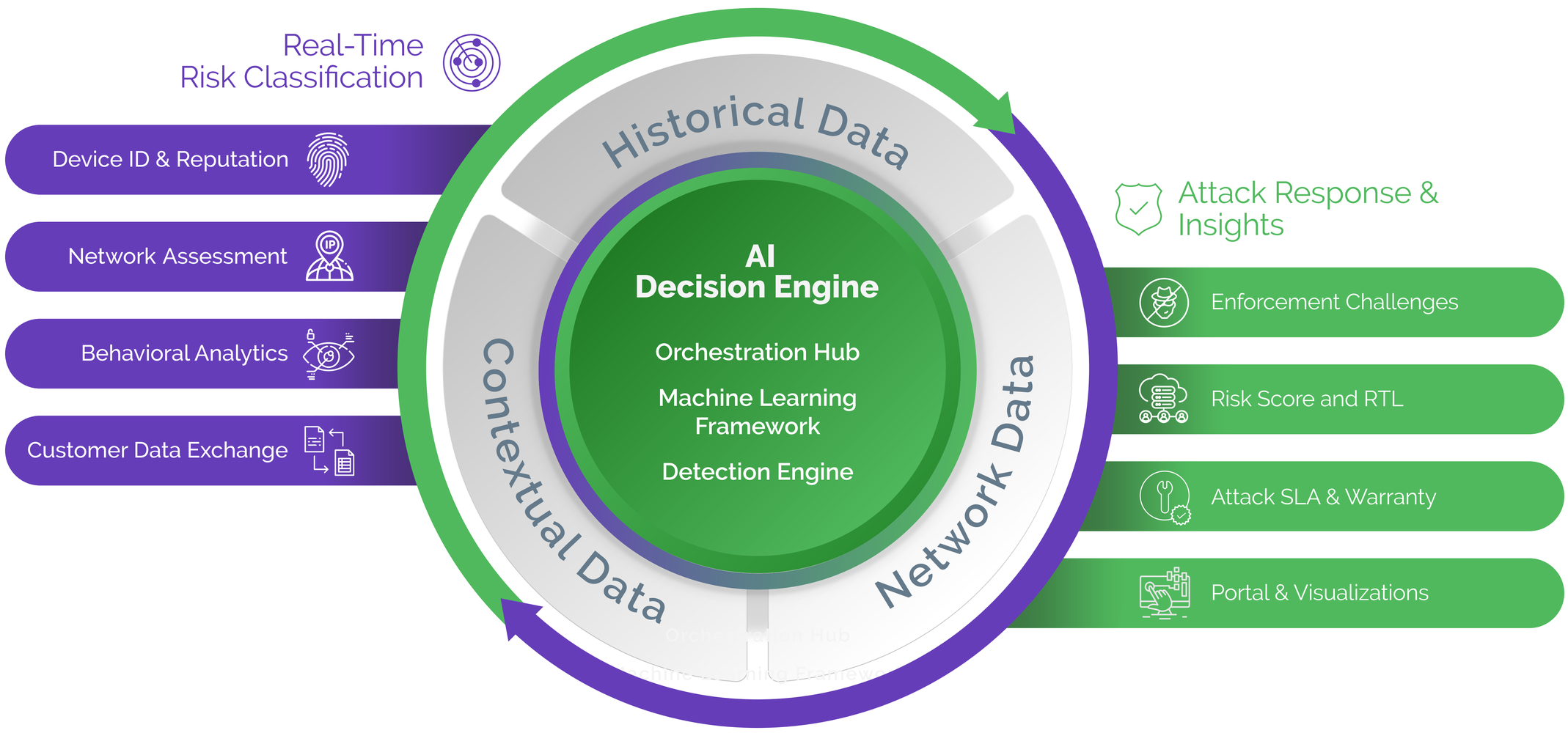
Carding and Gift Card Fraud
Detect large-scale testing of stolen payment credentials on checkout pages, and prevent fraudulent gift card purchases.

Abuse of P2P Marketplaces
Stop bot-driven abuse that disrupts the integrity of peer-to-peer marketplaces including fake reviews, fake listings, spam, and malicious content.

Loyalty Point Theft
Prevent fraudsters from breaking in to customer accounts in order to monetize accumulated loyalty points and rewards.

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 deters 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 continually orchestrate a targeted attack response. It continuously evolves from real-time assessments 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 behavior, while monitoring its 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 from tell-tale 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 break 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 are unable to solve. No off-the-shelf technology can be used to solve our challenges, forcing fraudsters to continuously build AI and waste time and resources.

Human Fraud 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 existing risk models.

Attack SLA & Warranty

Arkose Enforce deploys a foolproof acid test to stop bots in their tracks. 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 retailers 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.

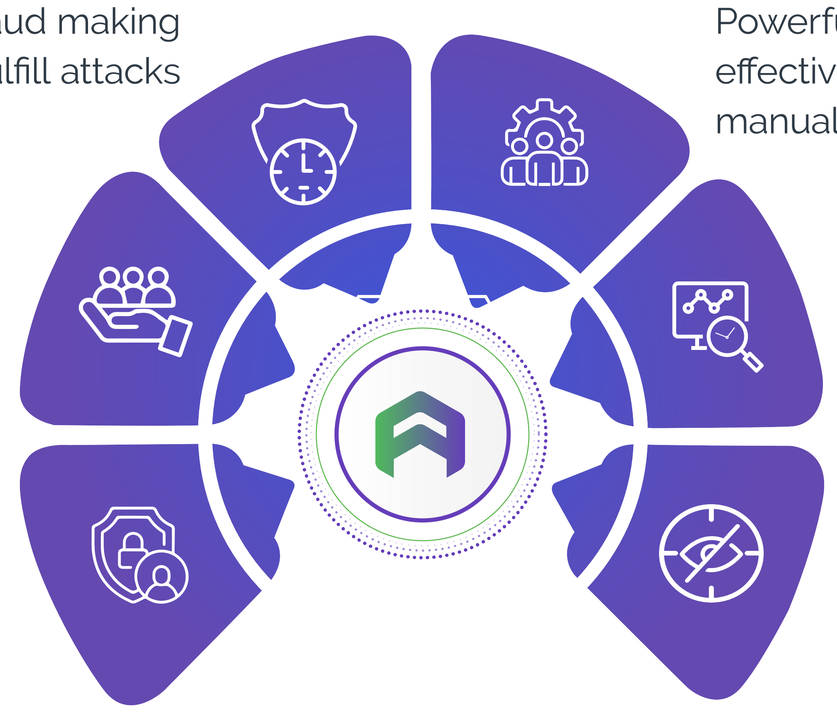
High-risk traffic is challenged, never blocked	Invisible screening means customers rarely see challenges	Flagged good users easily solve challenges on the first try	Challenge interaction data trains the decision engine	Improve user experience by reducing reliance on MFA

The Arkose Advantage

Long-term deterrence
Arkose Labs increases the cost of fraud making it economically unsustainable to fulfill attacks

Protection across the digital experience
One flexible solution that protects against different attack vectors across digial touchpoints

Privacy friendly
Arkose Lab technology achieves unparalleled accuracy without compromising data protection compliance



Effortless management
Powerful decision engine selects the most effective response strategy to reduce manual reviews

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

eComm Giant Beats Fake New Accounts

One of the world's largest ecommerce marketplaces was targeted by bots and humans fraud farms, to set up fake new accounts at scale.

Impact:

- Subcription promo abuse, fake reviews, and chargebacks
- Existing security measures were damaging good user experience

Results:

- 54% reduction in fake new accounts created
- No damage to good user throughput rates

Major Travel Site Slashes Bot Scraping

A major travel booking site had millions of bots scraping information daily, accounting for up to 75% of its traffic during attack peaks.

Impact:

- Damage to look-to-book ratio
- Bot volume put a strain on site's infrastructure

Results:

- 99% reduction in malicious bot traffic
- Look-to-book ratio increased from 1% to 6%

Gift Card Network Stops Card Testing

A premier distributor of prepaid cards and gift cards was targeted for card balance testing and attempts to redeem stolen cards.

Impact:

- Existing solution was being by passed by trained bots
- Poor user experience

Results:

- 98% reduction in bot attacks
- Improved good user experience

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