Arkose Labs | SOLUTION BRIEF

Arkose Labs for P2P Marketplaces

As in-person transactions declined through the pandemic, people around the world resorted to online shopping to reduce their exposure. Not only did e-commerce platforms boom during the pandemic, but online P2P marketplaces saw an uptick in activity as well with people finally having the time to purge unwanted goods, seek unique items for home projects, and line their pockets a little extra during hard times like these. Unfortunately, fraudsters saw this as an opportunity to line their pockets as well which ultimately hurt marketplace brand reputation and left companies with hefty repayment costs.

In order to uphold the integrity of the platform, P2P marketplaces are aiming to get ahead of scams that continue to occur, especially during the payment transaction flow. These scams are typically led by human fraudsters trying to come across as genuine users, making them difficult to catch. Online marketplaces bear the responsibility of protecting their users and providing the safest, most regulated way to buy and sell goods. Scams like selling broken items at full price, demand for advanced payment, and even SIM swaps ultimately fall on the company's shoulders, leaving them with high repayment costs. To prevent customers from falling victim to proliferating attacks, marketplaces need an effective solution to detect scams before they happen and prevent them from returning in the long-term.

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. Digital merchants choose 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

Fraudulent Profiles and Listings

Prevent fraudsters from setting up fake new accounts with stolen and synthesized identity credentials in order to create bogus profiles or marketplace listings to defraud users.

Protect P2P financial transactions

Safeguard consumer's financial credentials and protect your platform from malicious actors targeting P2P money transfer services to steal or launder money.

Account Takeover

Trust is key in P2P platforms; keep your customer accounts safe from being used maliciously through robust protection of the login page.

Spam & Phishing

Detect and stop large-scale abuse of messaging services in P2P platforms, targeted by bad actors to send malicious content

API Abuse

Prevent automated scripts from connecting directly to web or mobile facing APIs, posing as legitimate human traffic.

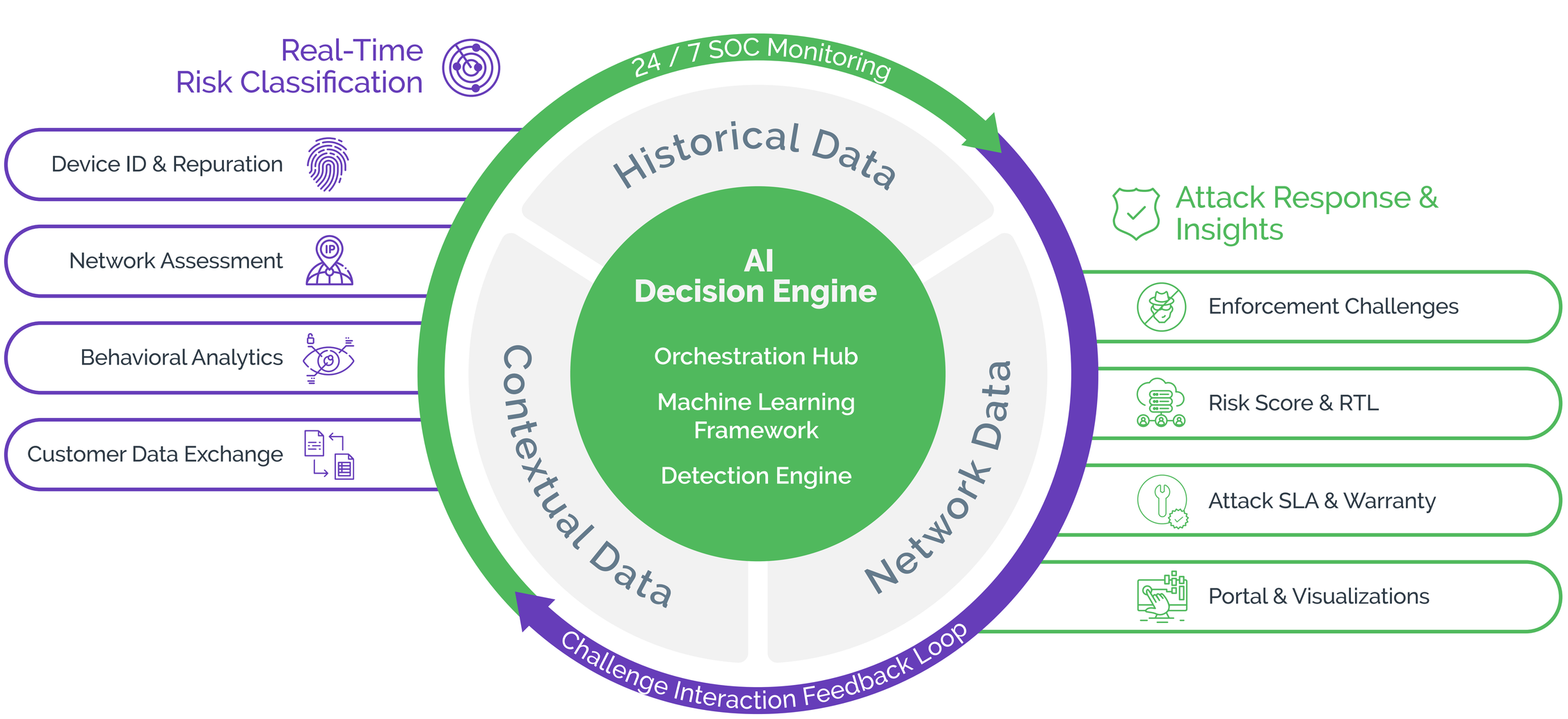
Fake Reviews

Ensure the integrity of the platform by preventing bogus reviews and bot-driven upvoting and downvoting.

The Arkose Labs Fraud Deterrence Platform

The Arkose Labs platform empowers security and fraud teams to root out large-scale, persistent attacks, with real-time risk classifications of traffic, powered by multi-faceted machine learning and 24/7 analysis from a Security Operations Center.

Unlike black box solutions, our “clear box” approach focuses on delivering actionable insights with clear explanations for risk classifications and a clear path to remediation. This goes beyond solutions that provide probabilistic risk scores, which often require a great deal of resource time to integrate, fine tune, and define downstream authentication workflows`. Our unique combination of risk classification and dynamic attack response delivers the appropriate pressure to the attack signature, while keeping disruption to legitimate users to a minimum.



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. It is continuously learning 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 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 and monitor integrity over time based on its characteristics and behavior. Works for desktop, browser, mobile apps, and smart TVs.

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 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.

Bots Defense

Suspected bot 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 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 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

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
Avoid high-cost authentication measures and downstream losses by opting for early screening methods

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

Arkose in Action

Social Media App Prevents 300M Spam Attacks a Month

One of the top 10 most downloaded social networking apps was receiving hundreds of millions of spam attacks every month. The app was favored by many for its largely unregulated registration web application, and more.

Impact:

- The client saw millions of spam messages which damaged their user experience
- Due to high amounts of abuse, legitimate activity decreased as customers left the platform

Results:

- Decreased 300M spam attacks in the first 30 days
- Automated attacks become untenable

Gaming Giant Stop Automated Attacks and Saved Millions of Dollars

The client is one of the world's largest sports video gaming companies that provides immersive, life-like gaming experience to its global user base.

Impact:

- In-game currency abuse through automated, bot-triggered sessions
- Auction house abuse to manipulate in-game economics

Results:

- Fifteen-fold reduction in fraudulent activity
- Eliminated in-game auction house and virtual currency abuse, saving the company millions of dollars

E-commerce Giant Stops New Account Fraud

The client operates one of the world's largest e-commerce platforms and connects millions of buyers and sellers globally

Impact:

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

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

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput. Based in San Francisco, CA with offices in Brisbane, Australia and London, UK, the company was honored as the 195th fastest growing companies in the United States on the 2021 Inc. 5000 list.

Email:
demo@arkoselabs.com

Schedule Demo