Arkose Labs | SOLUTION BRIEF

Arkose Labs for P2P Platforms

Trust is Key in Sharing Economy and P2P Platforms

P2P platforms are built on a foundation of trust. If those who use these platforms can't be sure who they are exchanging goods or services with are who they really say they are, then the entire model falls apart.

As the popularity of these platforms grows and expands across verticals including finance, lending, automotive, travel, work services, and more, fraudsters find more avenues to compromise user accounts or set up fake accounts, with the ultimate goal of monetizing attacks. Protecting users from such attacks and ensuring trust are critical to the continued growth of P2P platforms and the sharing economy.

Protecting the P2P Ecosystem from Fraud

Arkose Labs takes a new approach, one that focuses on long-term fraud deterrence rather than mere mitigation. We do this by bankrupting the ROI behind fraud, which compels fraudsters to stop attacking platforms protected by Arkose Labs. The Arkose platform protects all user interactions on P2P websites and apps using a combination of risk profiling and enforcement challenges.

Arkose Labs detects and deter attacks at user authentication points where account takeovers, fake new account creations, bonus abuse, spam, and phishing originate. By rooting out fraud early in the life cycle, you can ensure that the P2P and sharing economy ecosystem is free from malicious actors.

Fraud and Abuse Prevention for the P2P Platforms

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 consumers' 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.

Fake Reviews

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

Spam & Phishing

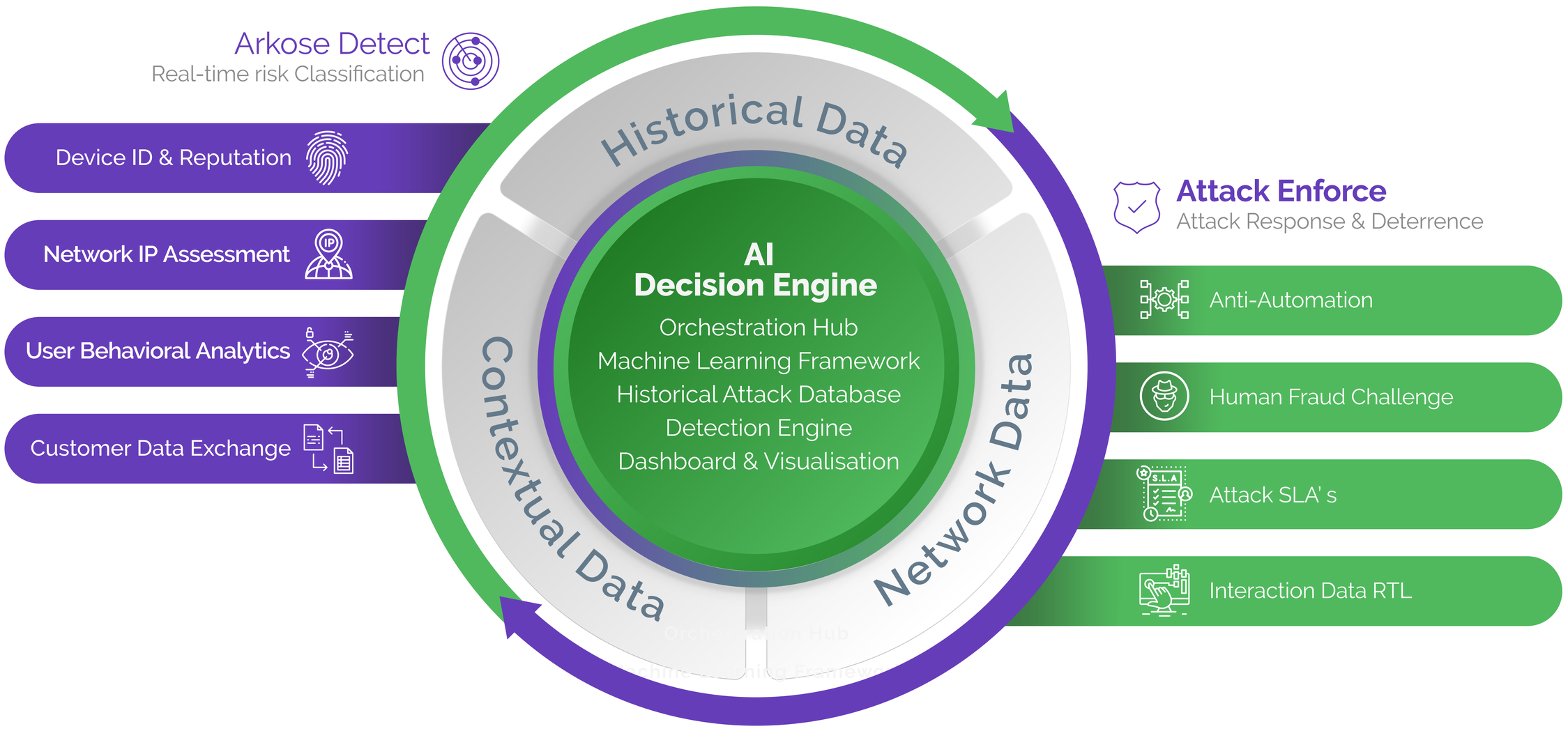
Detect and stop large-scale abuse of messaging services in P2P platforms, targeted by bad actors to send malicious content

API Abuse

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

Arkose Labs Fraud Deterrence Platform

Arkose Labs delivers long-term fraud and account security, 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 that deters future attempts, creating a more secure experience for genuine customers.



Arkose Decision Engine

Our AI-driven decision engine uses advanced analytics to confidently root out suspicious traffic, determine the appropriate attack response, and evolve models in real-time to rapidly adapt to threats.

AI-driven machine learning

Our advanced machine learning model evolves decisioning rapidly from real-time signals, historical attack patterns, and attacks across the Arkose Labs Global Network of customers.

Story-based detection

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.

Customer dashboards

Dashboards provide insight into ongoing mitigation efforts, including when new fingerprints and telltales have been added, when threats were detected, and historical trends. Detailed logs of user activity are provided to clients with rich insights including telemetry data, risk level, and information from across the network.

Arkose Global Network | Arkose Labs takes a consoetium 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

Arkose Detect assesses real-time device & behavioral intelligence to unearth malicious human traffic and classify suspicious traffic for enforcement, while legitimate users sail through.

Device ID & reputation

Deep device forensics is used to fingerprint devices based on its characteristics and behavior and monitor for 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 rerouting traffic through inexpensive 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 deliver more targeted attack response.

Arkose Enforce

Arkose Enforce delivers targeted attack response that break the economics of bot and human-driven attacks and makes them non-viable. User interaction data provides immediate insight and truth data on suspected malicious sessions.

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 and waste time and resources.

Human Fraud Defense

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.

Inclusivity & compliance

Our platform works in more than 100 languages, automatically displaying the language of the browser setting. Challenges are also Section 508-compliant with available audio and keyboard controlled challenges to be inclusive of people with varied abilities.

Intent validation & feedback

Challenge interaction data is fed back into the decision engine as instant truth data to validate the risk classification and further train machine learning models.

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.

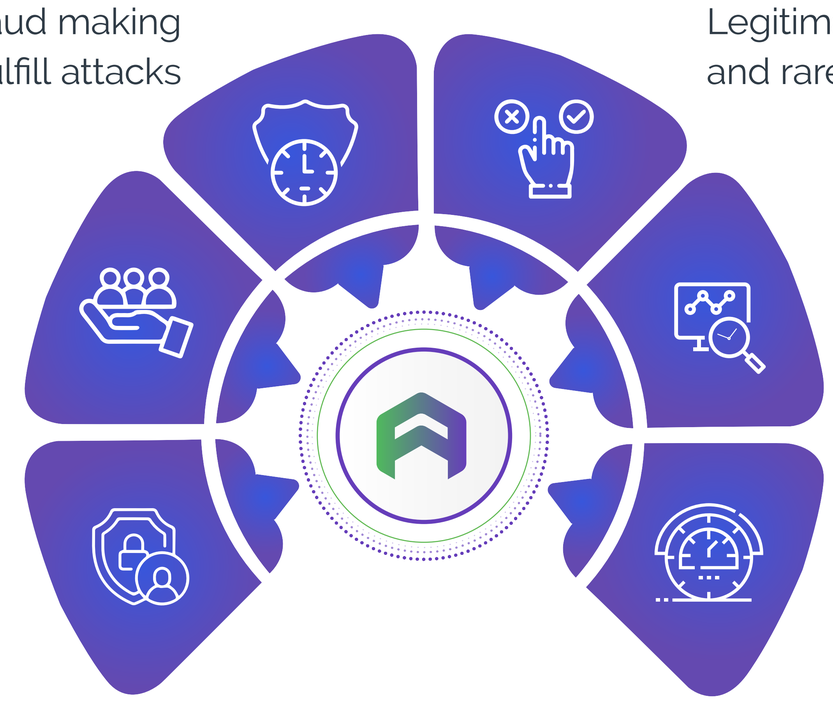
- High-risk traffic is challenged, never blocked
- Invisible screening means customers rarely see challenges
- Flagged good users easily solve challenges on the first try
- Challenge interaction data trains the decision engine
- Improve user experience by reducing reliance on MFA

The Arkose Advantage

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

Protection across the customer journey
One flexible solution that protects against different attack vectors and extensive user touchpoints

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



Solves the False Positive Conundrum
Legitimate consumers are never blocked and rarely experience user interdiction

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

Insurer Keeps Fraudsters Out of Claims

Targeted phishing attacks were carried out against customers by attackers pretending to be the client, saying they needed certain information about the insurance policy.

Impact:

- Fraudsters used stolen credential to submit false claims
- Users experience significantly disrupted, which harmed brand reputation

Results:

- Nearly all phishing attacks stopped after Arkose Labs was implemented
- No negative effect on user experience and significant uptick in customer retention

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:

- Targeted by account takeover attacks
- Sign-up process abused for account enumeration

Results:

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

Outlook.com Stops Fake New Account Creation

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

Impact:

- Fake new accounts created at scale
- Good users were being disrupted

Results:

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

> "Arkose Labs technology is an important component of our multi-pronged approach to minimize fraud without negatively impacting legitimate customers."
>
> **-Alex Weinert, Microsoft**

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