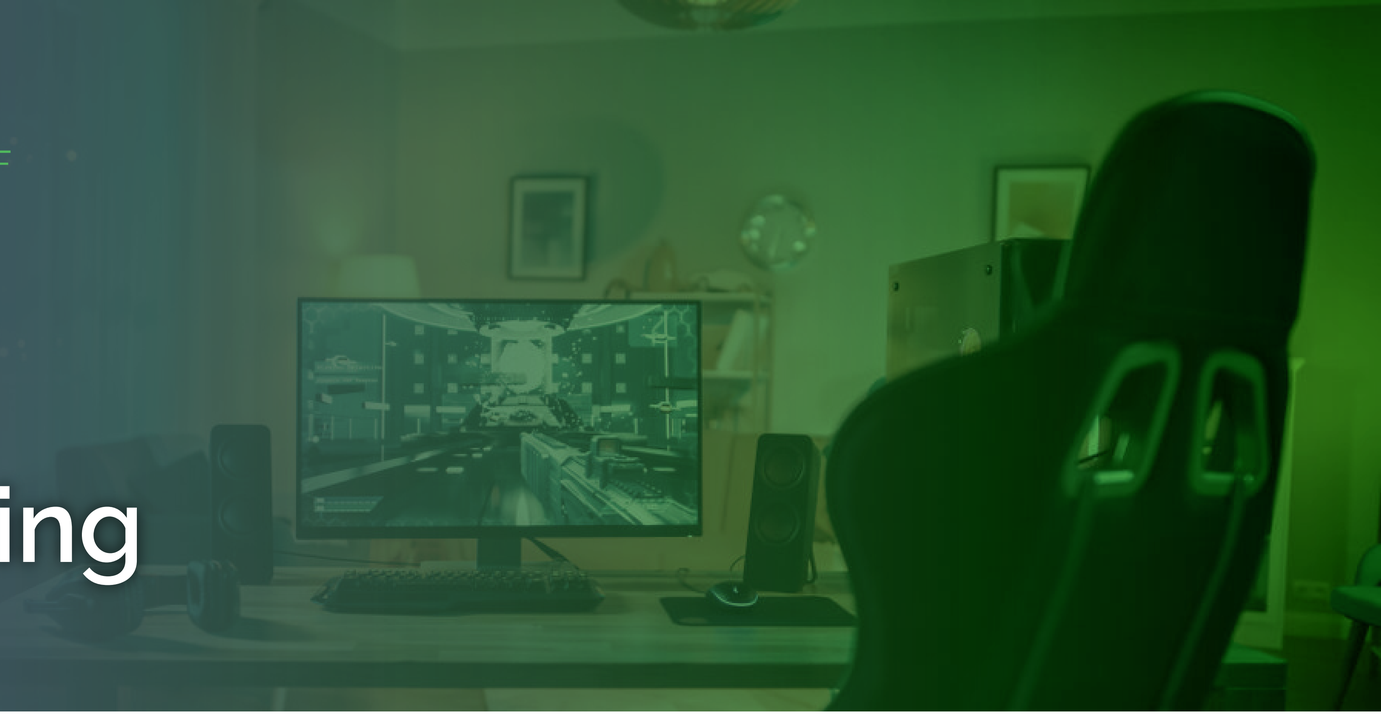
Arkose Labs | SOLUTION BRIEF



Arkose Labs for Gaming

Protect Your Gaming Arena from Sophisticated Fraud & Abuse

As time spent online exploded in the last year, every gaming platform has been hard at work attracting more users and increasing their share of players' game time. Unfortunately, record traffic volumes, sign up bonuses, and lucrative in-game economies have made games equally attractive for fraudsters to profit while hiding in plain sight. In fact, the gaming industry has seen unprecedented attack volumes since 2020 at a consistent attack rate of over 30%.

As demand surges, fraudsters will continue to target gaming platforms with complex attack patterns that mimic player behaviors. Fraud and security teams need solutions that decipher bots and human fraudsters from good players, without draining internal resources. One that delivers the ideal balance of blocking suspicious traffic without making players jump through hoops to prove their legitimacy.

Arkose Labs Bankrupts the Business of Fraud

Despite significant investments in fraud mitigation, gaming platforms are targets of fraud because financial incentive still exist. Arkose Labs bankrupts the business of fraud by sabotaging the ROI of large-scale bot and human-driven attacks until they're no longer profitable. This is a fundamental shift from fraud mitigation to fraud deterrence.

The world's most prominent gaming platforms trust Arkose Labs to eliminate account takeover losses, abuse of virtual economies, in-game cheating, and downstream banning. With powerful detection and targeted attack response tailored to bot and human-driven attacks, you can fight aggressively against fraud and in-game abuse without disrupting legitimate players.

Protection for the Most Targeted User Touchpoints

Credential Stuffing & Account Takeovers
Halt fraudsters from accessing genuine accounts to steal and resell players' hard-earned assets, or dormant accounts for in-game cheating.

Automated Attacks
Identify and prevent bots from initiating gaming sessions to collect virtual currency or assets without disrupting the gaming environment.

Spam & Abusive Behavior
Protect communication channels from phishing, spam, and malicious content.

Fake New Accounts
Prevent fraudsters from creating multiple new acccounts to receive new account bonuses, spam legtimate players, or conclude with other bad actors

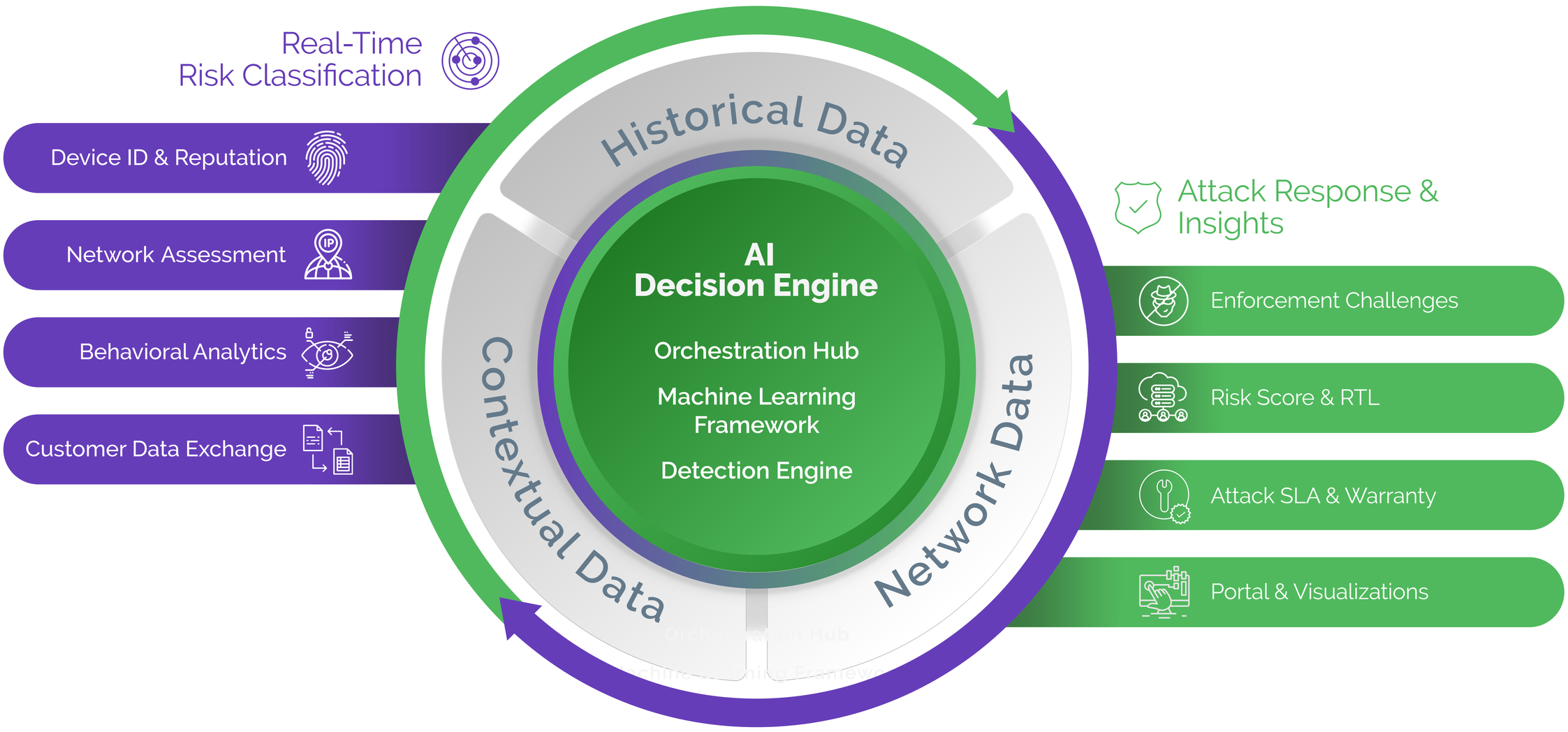
Real Money Trading
Secure the in-game experience from auction house abuse, economy inflation and match-fixing.

Bonus Abuse
Launch promotions and customer acquisition giveaways with robust protection in place to prevent bonus abuse.

> The difference between Arkose Labs and our past solution is night and day for us. Previous defenses created a bad user experience, while Arkose Labs solves the problem and makes it fun for our users.
> - Antoni Choudhuri, Roblox

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 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 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 and monitor integrity over time based on its characteristics and behavior. 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 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 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

Superior customer throughput
Targeted friction delivers 33% higher completion rate over MFA

Early detection & deterrence
Prevent fraudsters from creating multiple new accounts to receive new account bonuses, spam legitimate players, or collude with other bad actors.

Guaranteed bot protection
Identify and prevent bots from initiating gaming sessions to collect virtual currency or assets without disrupting the gaming environment.

Managed service support
Secure the in-game experience from auction house abuse, economy inflation and match-fixing.

Effortless management
Powerful machine learning models select the most effective response strategy while reducing manual reviews.

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

Arkose in Action

Gaming Giant Stops Bots, Saves Millions

Major sports video game platform implemented Arkose Labs to stop bot-driven game play, as well as account takeovers, that capitalized on their in-game economy.

Impact:

- Attackers resold virtual currency on the black market
- Disruption of fair play for genuine users

Results:

- 15x reduction in fraud activity
- Eliminated virtual currency abuse and saved millions

Roblox Thwarts Fake Account Creation

The user-generated game platform enlisted Arkose Labs to eliminate automated account creation aimed at manipulating game popularity.

Impact:

- Bot-generated games ranked over user-created games
- Redirection of genuine traffic off Roblox's site

Results:

- Significant reduction in fake users
- Added defense without impacting new account conversion

Game Platform Reduces Bots and Escalations

A popular game developer chose Arkose Labs to protect against thousands of daily bot attacks on logins and account registration.

Impact:

- Customer issues from account takeovers
- Increased customer escalations from false positives

Results:

- 60% reduction in attacks
- 84% decrease in support escalations

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.