Arkose Labs | SOLUTION BRIEF

Arkose Labs for Media & Streaming

Safeguard user accounts and protect revenue-generating content

As consumer engagement in online content and entertainment exploded, media and streaming platforms became veritable gold mines for fraud. Operating in a highly competitive landscape, it's already a race to capture every consumer dollar. The promotional offers and 'freemium' models aimed at attracting new customers are being exploited by fraudsters for their own financial gain. Disguised as legitimate users, fraudsters target these platforms to steal personal data, access content behind paywalls, snatch payment credentials, and disseminate spam to billions of potential victims. With attacks comprising 1 in 5 transactions on media platforms, in-house fraud teams need advanced mechanisms to weed out bad actors amidst increased traffic, while protecting users and revenue-generating content from being abused.

Arkose Labs Bankrupts the Business of Fraud

As long as there is profit to be made, fraudsters will continue to attack with increasingly sophisticated methods of mimicking legitimate users. Arkose Labs sabotages bot and human-driven attacks by targeting the economic incentive driving attackers to the point where they give up. This is a fundamental shift from fraud prevention to fraud deterrence. Digital media platforms trust Arkose Labs to detect and deter attacks at the most targeted user touchpoints where account takeover, fake account creation, scraping, and spam originate. A dual-pronged approach of dynamic attack response and targeted enforcement challenges allows media and streaming companies to better differentiate between legitimate and malicious activity, while maintaining the convenience and usability that they're known for.

Protection Against the Most Targeted Attack Patterns

Account Takeovers
Protect customer accounts from compromise and reselling of login and sensitive information.

Bonus Abuse
Protect profits by stopping fraudsters from abusing promotional offers meant to attract new customers.

New Account Fraud
Streamline the account sign-up process and prevent fraudsters from using stolen or fake user credentials to set up bogus accounts.

Scraping
Uncover fraudsters posing as genuine traffic in order to scrape data, content and images for malicious purposes.

Payment Fraud
Prevent fraudsters from accessing customer payment credentials or exploiting in-platform micro-transactions.

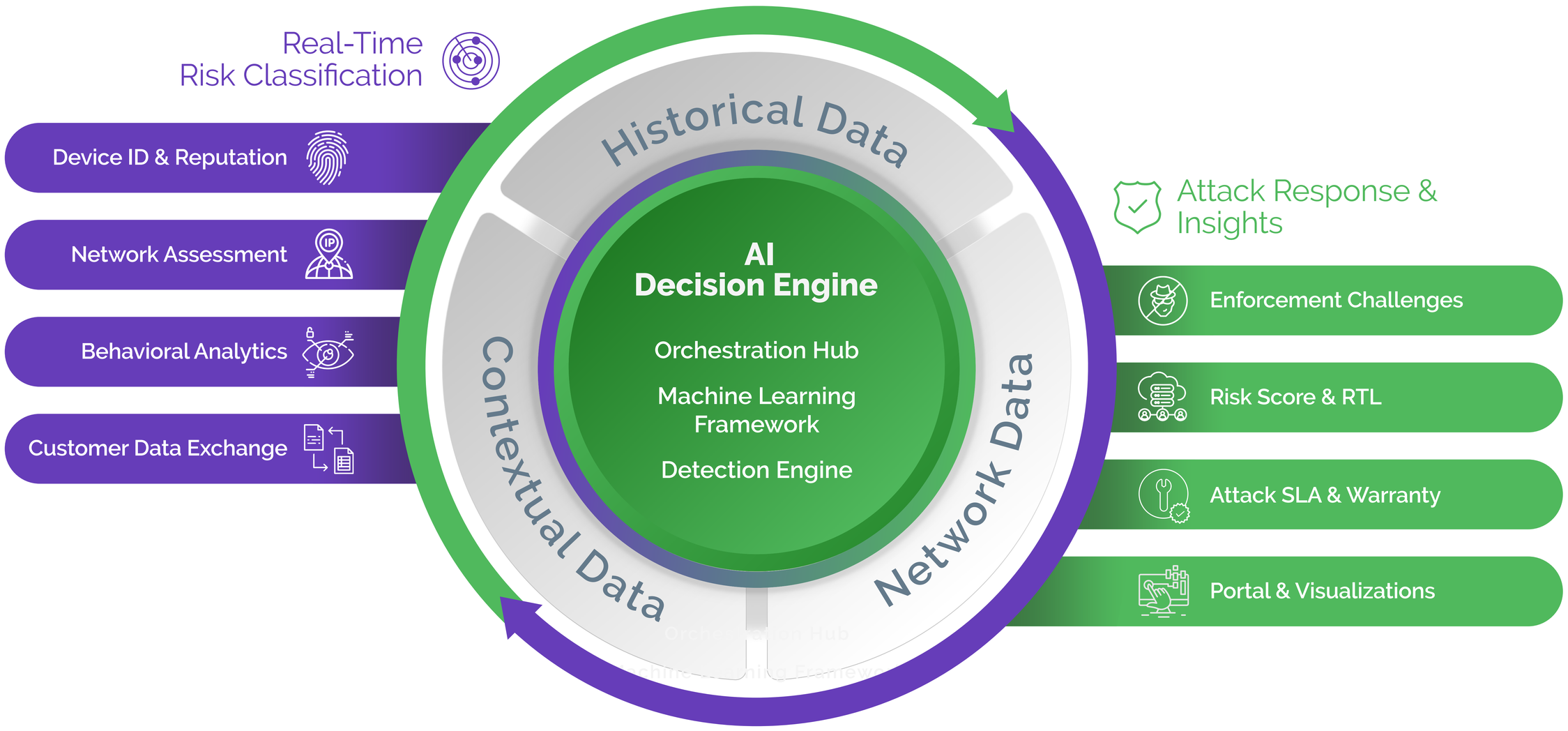
Phishing & Scams
Protect users from spam and scams, as fraudsters create fake profiles to try and manipulate good users.

Cross-device support for all digital media services

News | Video Streaming | Social Media | Dating | Mobile apps | Smart TVs

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, 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

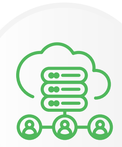
When traffic is flagged as suspicious, Arkose Enforce provides secondary screening and targeted attack response that break the economics of bot and human-driven attacks. Challenges collect user interaction data to further validate the user's intention and deliver truth data back to the decision engine.

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

User-centric security
Invisible screening means legitimate consumers are never blocked and rarely experience interdiction

Early detection & deterrence
Stops attackers at early user authentication points to diminish spam and payment fraud

Guaranteed bot protection
Robust bot defense backed by a 100% SLA guarantee and industry-first credential stuffing warranty

Managed service support
Arkose Labs works as a true partner in delivering fraud insights and curb repeat attacks

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

Social Network Reduces Scraping

A major social networking site was being hit with large-scale bot attacks, scraping public profile info from real users.

Impact:

- Difficulty differentiating between legitimate and malicious users
- Dissemination of user information deprived the platform of potential revenue

Results:

- 22% reduction in scraping
- 19% uplift in good user throughput
- Protected millions in potential revenue loss

Caffeine.tv Kicks Bots Out of Streaming

ReCAPTCHA, the live streaming platform's defense protocol, was being bypassed by bots creating new accounts en masse.

Impact:

- Dormant accounts were activated to disrupt service and interfere with live streaming
- Dissemination of spam damaged the experience for good users

Results:

- Eliminated all bot activity
- Stopped takeovers of dormant accounts

Dating Platform Ghosts Lone Fraudsters

A major dating site was targeted by human fraudsters who created fake accounts and compromised dormant accounts to scam users.

Impact:

- Users were spammed with malicious links and phishing schemes
- Difficulty identifying human-driven fraud before spam occurred

Results:

- Caught 80% of fake accounts before messages were sent to users
- Diminished downstream spam and abuse

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.