Arkose Labs | SOLUTION BRIEF

Arkose Labs For Tech Platforms

Making Cloud-Based Platforms Safe for All Good Users

Cloud-based tech platforms are a critical part of the global digital economy. They connect people from around the world and allow them to collaborate, share files, and work in an efficient and centralized manner. With millions of users on these platforms, it's no surprise that fraudsters flock to them as well.

From work, school, collaboration, and even social gatherings, tech platforms are indispensable to our modern lives. Yet fraudsters target user accounts as a gateway to take advantage of free server time, hack into video calls to spread malicious content, share malware, or much more.

Protecting Tech Platforms and Their Customers From Fraud

Arkose Labs bankrupts the business of fraud by sabotaging attackers' ROI and making it uneconomical to attack your business. This is a fundamental shift from fraud prevention to fraud deterrence.

No cloud-based tech platform can be successful if its users doubt that their data and information is safe on it. Arkose Labs offers peace of mind in this regard, with a unique approach that tackles human-driven and automated fraud and abuse. A combination of risk-based and step-up authentication, through innovative visual challenges, stamps out fraud on tech platforms - while enhancing good user experience.

Stop Fraud Against Tech Platforms Including:

New Account Registration
Prevent fraudsters from creating new accounts at scale with the intention of abusing the platform for illegal activities.

Account Takeover
Safeguard user accounts from ATO attacks and fraudsters carrying out large-scale credential stuffing attacks to hack into user accounts.

Spam & Phishing
Stop fraudsters from using bogus or hacked accounts to send spam and other malicious content at scale, aiming to scam users out of money or sensitive credentials.

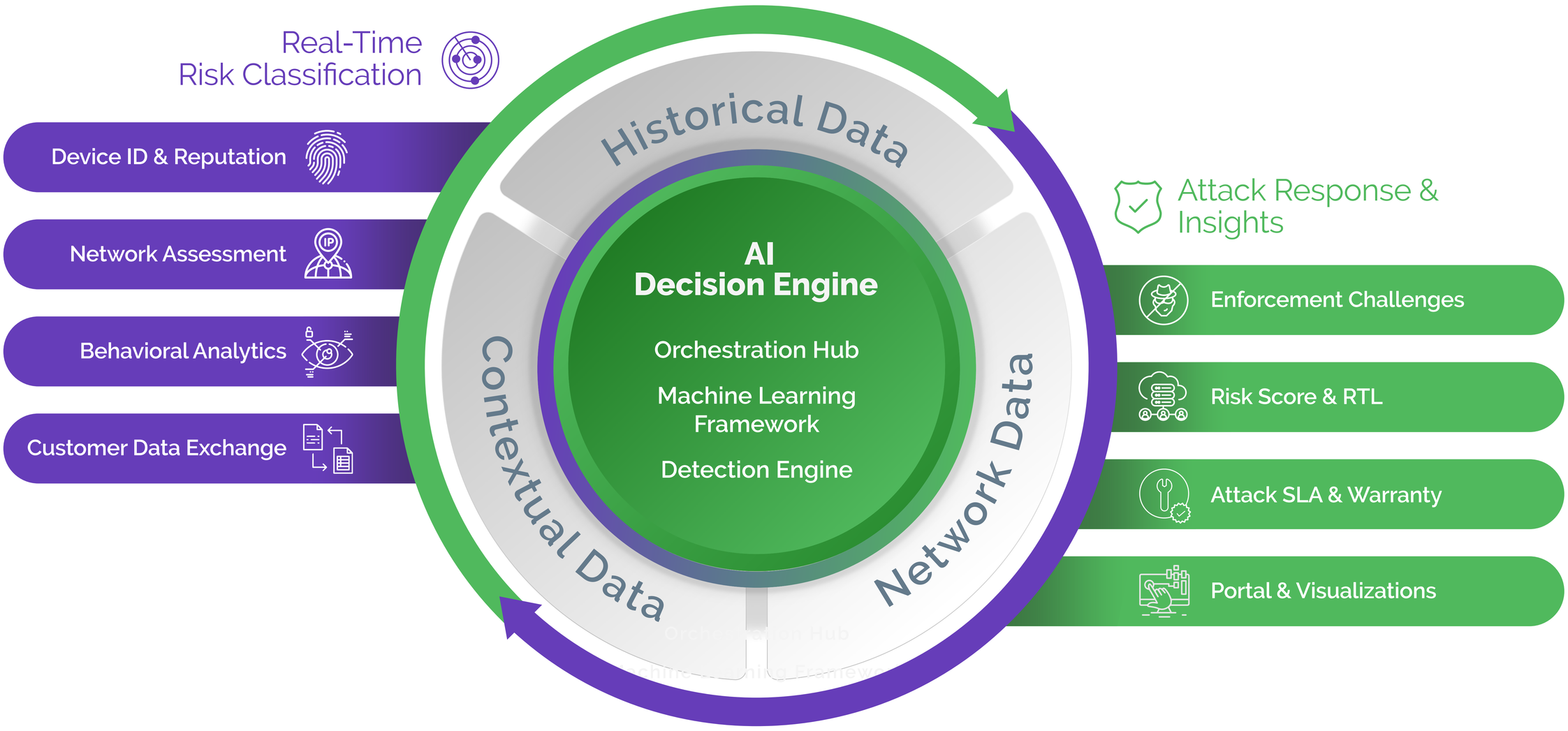
Web Scraping
Prevent attackers from stealing content and user data through high velocity, malicious scraping attacks.

Bonus Abuse
Launch promotions to entice new customers with confidence, by preventing fraudsters from taking advantage in order to get sign up credits or free access to platforms.

Secure Communication Channels
Secure communication channels from malicious actors looking to target sensitive commercial information or important files shared on tech platforms.

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

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.

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

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, mouse tracking, and page familiarity are used to distinguish good user behavior from malicious human traffic

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: 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 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 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 risk models.

Attack SLA & Warranty

Arkose Enforce deploys a fool-proof 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

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 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

Cloud Provider Stops Crypto Miners

A global cloud computing provider had an issue with human fraudsters creating fake new accounts to mine cryptocurrencies using free server time.

Impact:

- Fraudsters strained server capacity with high-compute crypto mining
- Severe cluster failures kept the team working overtime

Results:

- 95% reduction in attacks
- No damage to good user throughput rates

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:

- Sign-up process abused for account enumeration
- Existing solution created too much friction for users

Results:

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

Microsoft Outlook.com Tackles Fraud & Abuse

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

Impact:

- SMS tokens were expensive and circumvented by attackers
- Customer throughput was also impacted by SMS

Results:

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

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.