Arkose Labs | SOLUTION BRIEF

Arkose Labs for Travel

Throughout the past year, demand for travel has seen many ups and downs. With destinations around the world starting to reopen, the travel industry is experiencing a major comeback with everyone jumping at the opportunity to account for all travel, not just vacations, However, with an uptick in traffic comes at a cost as fraudsters and bots are relentlessly trying to sabotage businesses.

With the prevalence of scraping and other nuanced attack strategies being difficult to detect, companies are seeing an impact on revenue opportunities and customer conversion rates. With fraudsters constantly finding new ways to slip through the cracks, travel companies need a powerful, future-proof fraud deterrence system to help them take this spike in demand like a champ.

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 companies in our network. This is a fundamental shift from fraud prevention to fraud deterrence.

Global travel companies trust Arkose Labs to detect and deter attacks at user authentication touchpoints where loyalty and payment fraud, scraping, and fake reviews originate. By rooting out fraud early, companies are able to protect conversion rates, regain control over inventory, and maintain a positive user experience to keep customers coming back.

Protection for the Most Targeted User Touchpoints

Account Take Over

Prevent fraudsters from taking over genuine users' accounts to make fraudulent transactions

Payment Fraud

Shut down fraudsters using stolen credit card credentials to pay for bookings on your platform

Scraping

Stop fraudsters from stealing user data and inventory in order to sell to competitors

Fake Reviews

Protect brand reputation and promote honest feedback from your true customers

Inventory Hoarding

Take back the control over hoarded plane seats and vacancy to prevent unfair reselling of your inventory

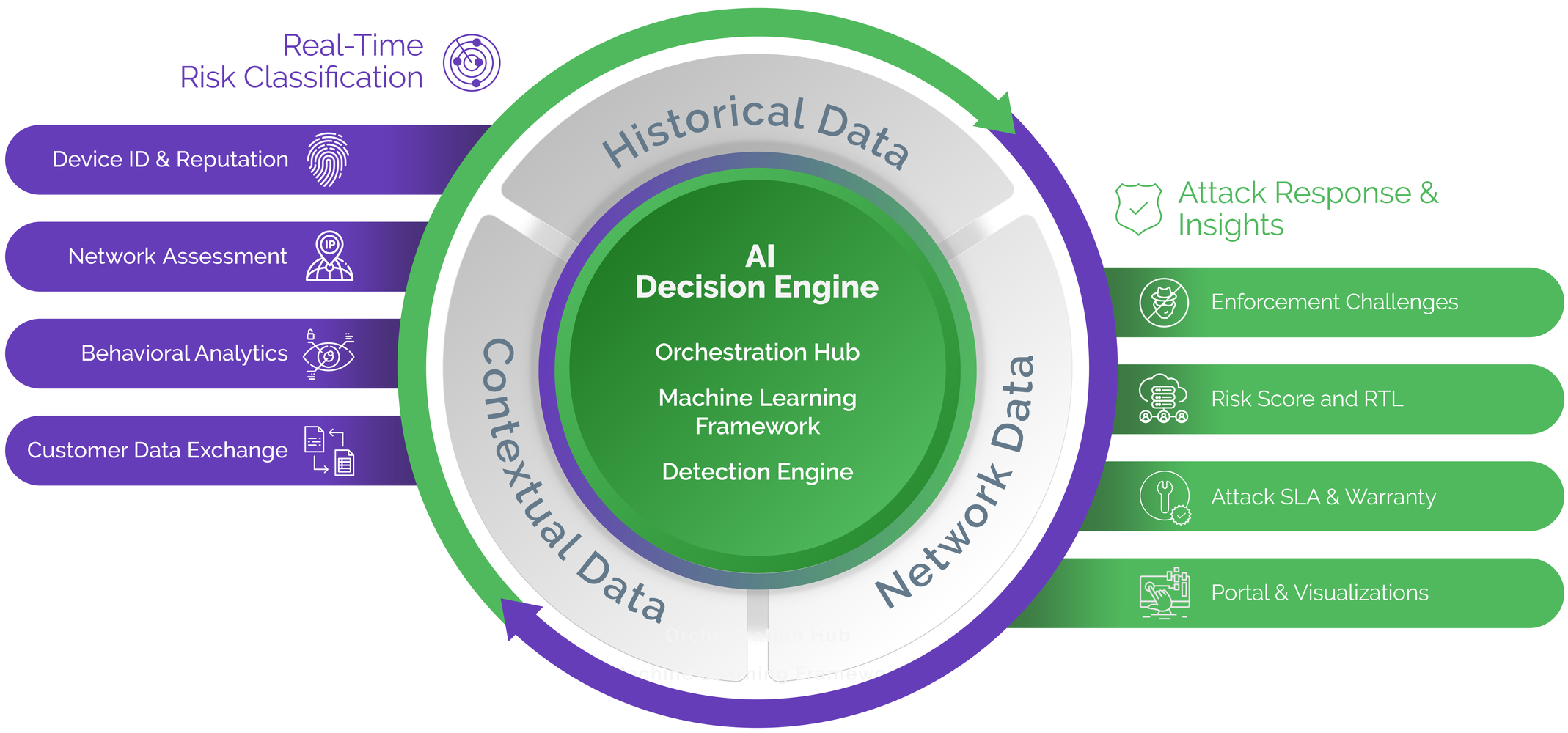
Loyalty Fraud

Stop fraudsters from taking advantage of loyalty offers and stealing accounts with accumulated rewards to later resell

© 2021 Arkose Labs. All rights reserved.

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 continually orchestrate a targeted attack response. It continuously evolves 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.

© 2021 Arkose Labs. All rights reserved.

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 based on its characteristics and behavior, while monitoring 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 cheap IP addresses.

User Behavioral Analysis

Behavioral biometrics such as keystroke, gyroscope, and page familiarity are used to distinguish good user behavior from tell-tale 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.

Bot Defense

Suspected bots are presented with a deep bench of challenges that machines are unable 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.

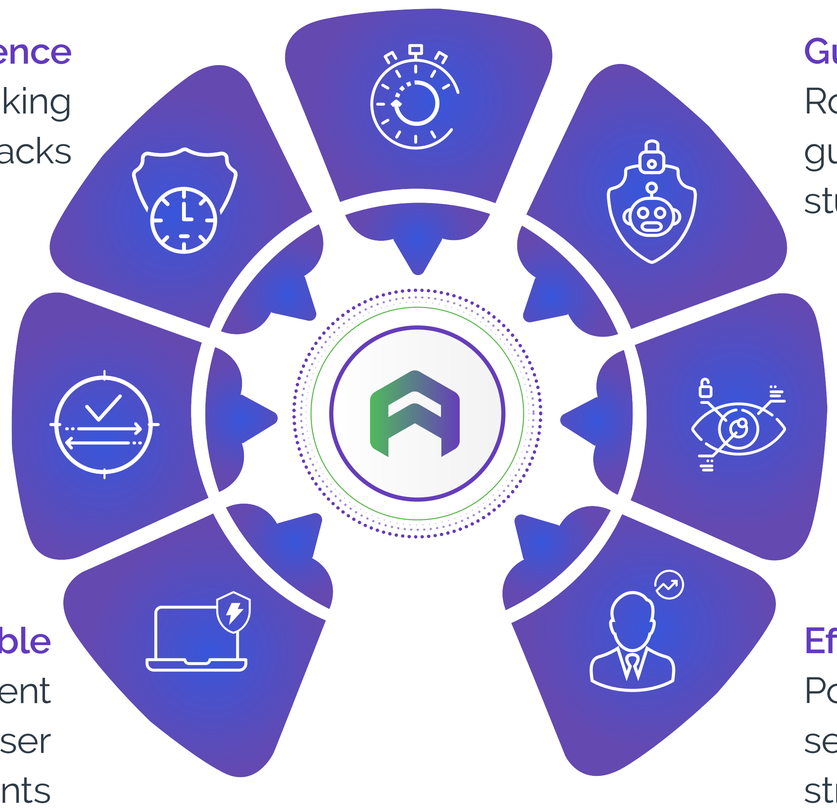
High-risk traffic is challenged, never blocked	Invisible screening means customers rarely see challenges	Flagged good users easily solve challenges on the first try	Challenge interaction data trains the decision engine	Improve user experience by reducing reliance on MFA

© 2021 Arkose Labs. All rights reserved.

The Arkose Advantage

Real-time response
Adaptive challenges root out automated attacks and sap fraudsters' time and resources

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



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

Minimum friction
Unified workflow brings together the detection and the proprietary challenge. The lower the risk is, the easier is the challenge

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

Flexible & adaptable
One solution that protects against different attack vectors and extensive user touchpoints

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

Arkose in Action

Major Travel Booking Site Eliminates Scraping

This major travel site was targeted by millions of bots per day scraping user information to later resell or publish for free use.

Impact:

- Value depletion for site information that benefits competitors
- Caused for poor standing and revenue loss

Results:

- Malicious bot traffic reduced by more than 99%
- Look to book ratio increased from 1% to over 6%

HK Express Prevents Inventory Hoarding Attacks

HK Express saw many inventory hoarding attempts leaving the business unable to sell large amounts of airplane seats.

Impact:

- Automated hoarding attacks made inventory unavailable to true customers
- Caused a decrease in bookings and loss of revenue

Results:

- 100% reduction in inventory denial attacks
- Due to fast implementation, bookings and revenue increased immediately

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.