Arkose Labs | SOLUTION BRIEF

Arkose Labs for Healthcare

The healthcare industry tends to be an unforeseen target for fraud in today's digital world. However, fraudsters are highly motivated to attack businesses in healthcare due to stolen medical records, billing data, and insurance details being some of the most expensive data on the dark web. If an attack is successful in this sector, the return for one single attack is much higher than in other industries.

Unlike other industries, healthcare companies have legal pressure to maintain maximum privacy for their clients, making effective fraud solutions a necessity. Protect sensitive information and avoid downstream abuse by preventing attacks and improving account security. Taking these strides in fraud prevention will enhance user trust and help meet HIPAA standards.

Arkose Labs Bankrupts the Business of Fraud

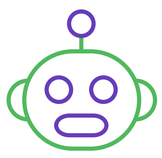
As long as there is profit to be made, fraudsters will continue to attack. Arkose Labs bankrupts the business of fraud by sabotaging attackers' ROI and making it uneconomical to attack you. This is a fundamental shift from fraud prevention to fraud deterrence.

Global healthtech and insurance companies trust Arkose Labs to detect and deter attacks at user authentication touchpoints where account takeovers, payment fraud, credential stuffing, and fake account creation attacks originate. By rooting out fraud early, companies are able to strengthen relationships with customers by offering an increasingly secure financial platform without sacrificing a positive user experience.

PROTECTION FOR THE MOST TARGETED USER TOUCHPOINTST

Credential Stuffing

Protect user accounts against credential stuffing and account takeovers, which puts users' sensitive medical records, billing, and insurance information at risk.



Bots & Abuse

Prevent fraudsters from using the platform fraudulently to perpetuate scams surrounding medical diagnoses and other private information.

Insurance Fraud

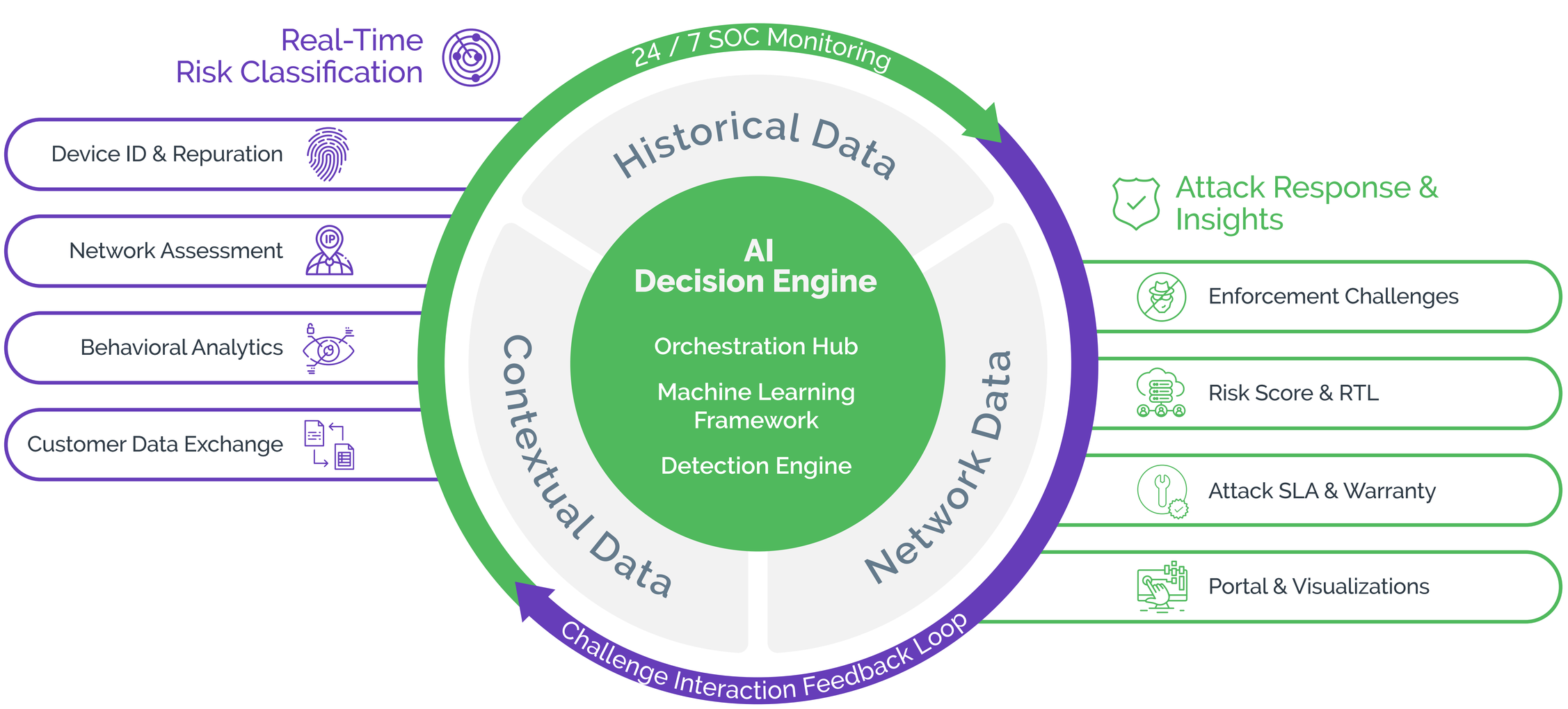
Accurately protecting clients from fraudsters using stolen insurance and billing information to be later used to obtain medical and dental care.

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.

The Arkose Labs Fraud Deterrence Platform

The Arkose Labs platform empowers security and fraud teams to root out large-scale, persistent attacks, with real-time risk classifications of traffic, powered by multi-faceted machine learning and 24/7 analysis from a Security Operations Center.

Unlike black box solutions, our “clear box” approach focuses on delivering actionable insights with clear explanations for risk classifications and a clear path to remediation. This goes beyond solutions that provide probabilistic risk scores, which often require a great deal of resource time to integrate, fine tune, and define downstream authentication workflows`. Our unique combination of risk classification and dynamic attack response delivers the appropriate pressure to the attack signature, while keeping disruption to legitimate users to a minimum.



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 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.

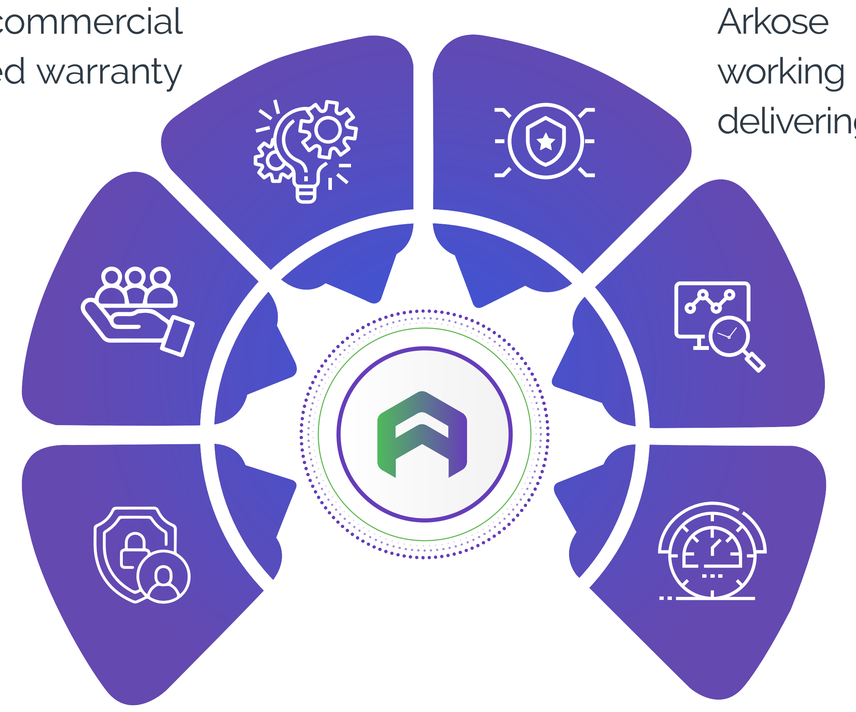
- High-risk traffic is challenged, never blocked
- Invisible screening means customers rarely see challenges
- Flagged good users easily solve challenges on the first try
- Challenge interaction data trains the decision engine
- Improve user experience by reducing reliance on MFA

The Arkose Advantage

Guaranteed Efficacy
Powerful protection backed by commercial assurance and industry-first limited warranty

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

Privacy Friendly
Arkose Labs technology achieves unparalleled accuracy without compromising data protection compliance



Managed Services
Arkose Labs empowers your teams by working as a true partner in fighting fraud and delivering insights specific to your business

Early detection
Avoid high-cost authentication measures and downstream losses by opting for early screening methods.

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

Arkose in Action

Healthtech Firm Protects Customer Data

The client is a major healthtech company that offers a digital health savings account (HSA) that works alongside HSA compatible plans, with an aim to make navigating healthcare easier for everyone.

Impact:

- The company was targeted by frequent bot attacks that used ATO to compromise customer data which damaged relationships and violated privacy standards
- The previous fraud solution used tactics like rate limiting and blocking which impacted the user experience where good users were getting locked out of their accounts.

Results:

- Nearly 1,000 attacks were thwarted per day
- This saved the company upwards of $1,500 per day
- User privacy was not impacted, keeping the company compliant

E-signature Company Protects Sensitive Digital Documents

The client is one of the world's leading e-signature and document workflow services. It serves hundreds of millions of users around the globe, who trust and rely on it to provide a safe and secure platform for signing and storing important digital documents.

Impact:

- Credential stuffing attacks targeted user accounts causing identity theft through stolen personal information
- The user experience was being disrupted by continual bot attacks, painting the illusion that sensitive information was not being secured properly

Results:

- Immediate drastic decrease in attacks
- No impact to good user throughput

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput. Based in San Francisco, CA with offices in Brisbane, Australia and London, UK, the company was honored as the 195th fastest growing companies in the United States on the 2021 Inc. 5000 list.

Email:
demo@arkoselabs.com

Schedule Demo

© 2021 Arkose Labs. All rights reserved.