

Arkose Labs for Telco

Telecommunications is the highway that connects billions of people across the globe. Today people rely on telco providers for more than just a mobile service. Connecting consumers to even more services like credit cards, WiFi, home security, entertainment, and more, telco accounts are increasingly more attractive to attackers.

With the prevalence of ATOs, identity theft, and more, telco fraud and security teams are faced with the challenge of protecting the company from massive fraud losses and accounts from being compromised. Combating persistent sophisticated bots and human driven attackers requires an adaptable approach that evolves with attacks and provides a user-centric authentication experience.

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 companies 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 TOUCHPOINTS



Account Takeover

Protect user accounts against credential stuffing and account takeovers, which puts users' critical financial and personal information at risk.



Fake Reviews

Eliminate fake reviews in order to prevent damage to brand reputation and create an honest feedback environment.



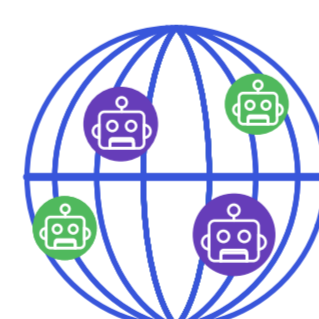
SIM Swaps

Improve user experience and customer relationships by preventing sim swap attacks that aim to steal and exploit mobile services.



Bonus Abuse

Prevent attackers from taking advantage of bonuses and rewards offered to loyal customers.



Large-scale Attacks

Avoid embarrassing headlines and keep to compliance standards by eliminating large-scale automated attacks aiming to steal customer data.



Mobile Abuse

Adopt an anti-fraud solution that effectively mitigates and deters attacks from a wide range of devices.

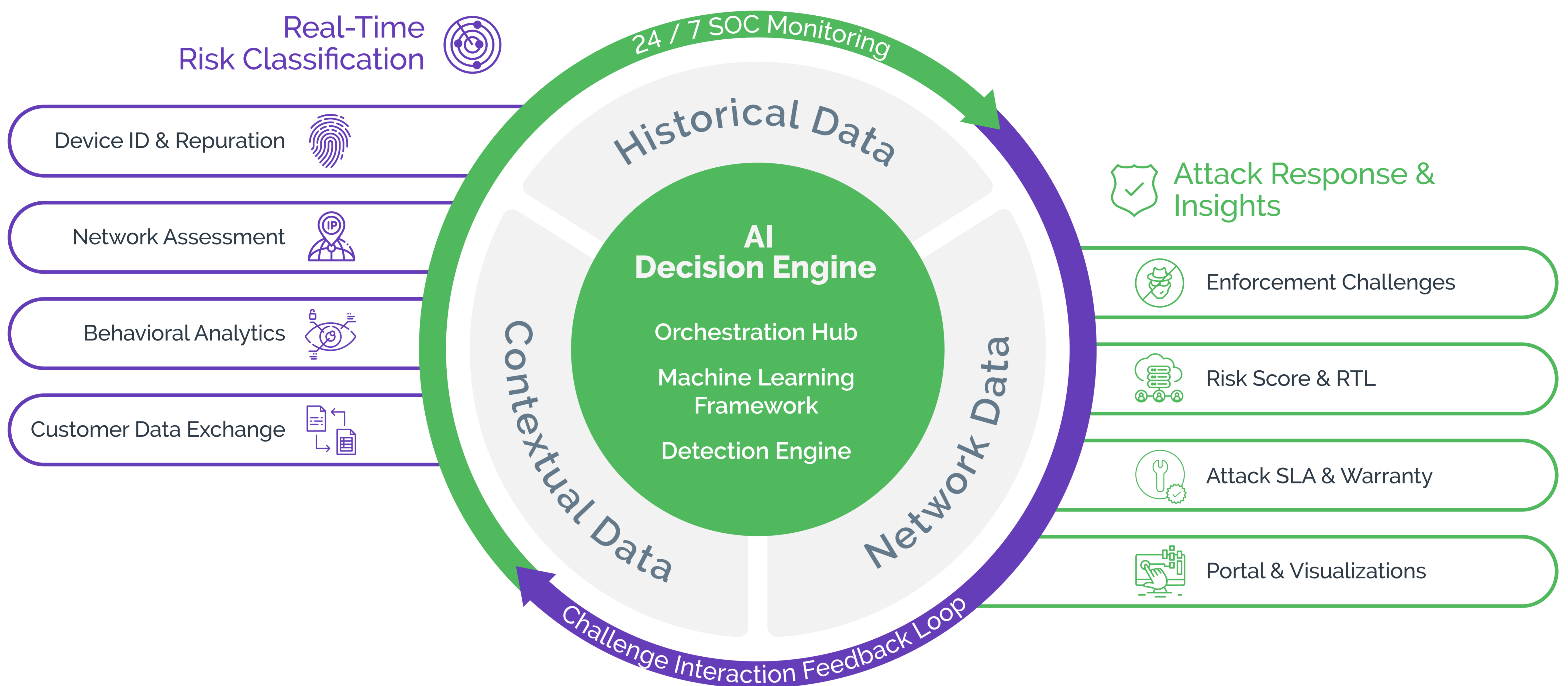
Arkose Global
Network

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.



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

Results fast

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



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.

Privacy Friendly

Arkose Labs technology achieves unparalleled accuracy without compromising data protection compliance

Arkose in Action



Fintech Neobank Beats ATOs

One of the world's most prominent fintech firms was targeted by bots executing credential stuffing attacks at scale. Successful attacks lead to the draining of customer funds and poor user experience.

Impact:

- Appeared untrustworthy to customers and damaged overall relationships
- High repayment costs as a result of ATOs

Results:

- 75% reduction in ATO attempts
- Slashed compromised account costs previously hitting \$100,000 per week



Microsoft Outlook.com Tackles Fraud and Abuse Globally

Outlook.com has hundreds of millions of active users and is trusted to provide secure communication; however, its popularity makes it a prime target for fraudsters looking to abuse new accounts.

Impact:

- Large-scale fake account registrations to use for blackmailing individuals with unfounded threats of revealing compromised information to their contacts.
- Previous fraud solutions failed to address the problem while remaining costly to the business.

Results:

- 33% improvement in good customer throughput



E-commerce Giant Stops New Account Fraud

The client operates one of the world's largest e-commerce platforms and connects millions of buyers and sellers globally.

Impact:

- The client struggled with bots and human sweatshops creating fake new accounts which were used to commit numerous types of downstream abuse.
- Efforts to quell fraud were degrading the user experience for good customers and remained ineffective at stopping these attacks.

Results:

- 54% reduction in fake new accounts created
- Significant reduction in downstream abuse

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

© 2021 Arkose Labs. All rights reserved.

[Schedule Demo](#)

© 2021 Arkose Labs. All rights reserved.