Arkose Labs | SOLUTION BRIEF

Bankrupt the Business Model of Fraud and Abuse with Arkose Labs

Overview

The digital economy is built on trust and powered by data. When a user creates an account, makes a payment, or accrues reward points-it's not just an exchange of goods or services, it's a transaction in the ultimate currency: trust. As companies become increasingly connected in the digital economy, the value of data hinges on how it can be harnessed to make decisions.

Recent breaches have provided abundant data to bad actors. Motivated by economic incentives, they use tools and techniques to subvert risk assessments with stolen identities and sophisticated technology that disguises inauthentic intent. Traditional prevention are no longer effective countermeasures and increase friction for good customers. Companies need a solution that undermines the long-term economic viability of fraud while delivering an unrivaled customer experience.

Businesses Need a Better Way to Manage Risk

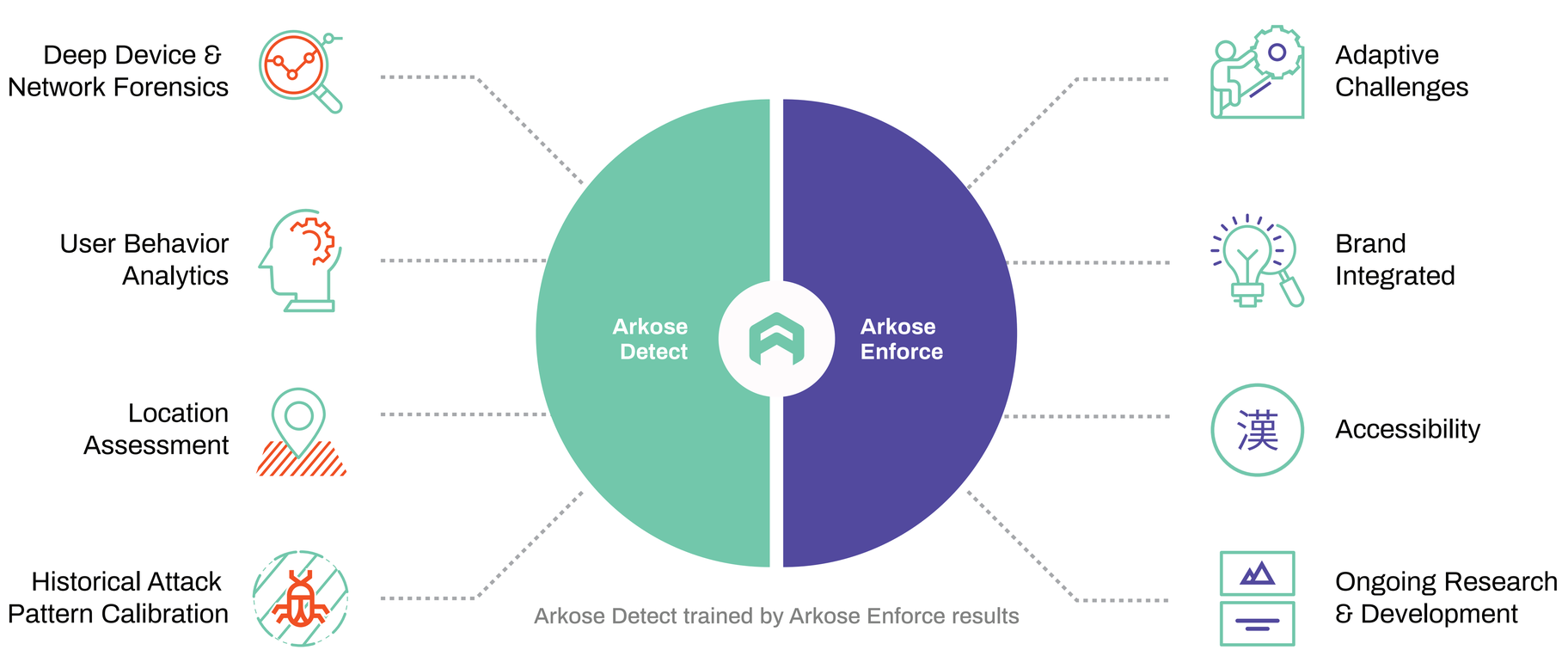
Today's economic climate has fostered favorable operating conditions for attackers. Innovation in the developing world has commoditized previously out-of-reach technology and provided fraudsters with affordable resources to attack companies for quick financial gain. No matter how small or invulnerable it seems, bad actors race to monetize every stage of the customer journey with fraud. Attack innovation has not only changed the scale and frequency of fraud, but also the complex ways in which it is committed–such as through human-powered click farms that imitate good customer data and avoid detection.

Current approaches in fraud and abuse prevention rely on data that attackers can manipulate. They are able to use inexpensive tools and abundant identities to emulate good customers, which increase false negatives and make them exponentially harder to detect without blocking.

The Arkose Labs Fruad and Abuse Prevention Platform

To effectively manage fraud and abuse in this rapidly evolving ecosystem, businesses need a long-term approach that evolves with attack patterns. Since abuse can only be sustained when the incentive outweighs the cost, companies need a solution that makes attacks economically irrational for fraudsters without introducing friction for customers.

The platform combines Arkose Detect (dynamic risk engine) with Arkose Enforce (adaptive step-up) to seamlessly differentiate good customers from bad actors. This proprietary approach evolves as attack pattern changes and diminishes the profitability of attacks.



Arkose Detect

Arkose Detect is a dynamic risk engine that invisibly analyzes transaction through a layered approach that looks at multiple parameters in real time. Key features of Arkose Detect include:

Deep Device and Network Forensics

Advanced methods investigate and profile the obscured identity of each attack

User Behavior Analytics

Historical insights from past interactions break users into smaller groups with distinct underlying motivations

Location Assessment

Origin of attacks are determined and then shared across the platform through network effect

Historical Attack Pattern Calibration

Network intelligence from years of global abuse evaluates attack patterns and the interplay of manual and automated tactics

Arkose Enforce

Arkose Enforce is an adaptive step-up that disrupts the monetization of attacks with challenges that don't impact good customers. Key features of Arkose Enforce include:

Machine and Human-Specific Challenges

Preventive techniques automatically adapt to prevent both machine and human-powered attacks

Branded Challenges

Customer experience can be visually customized to champion the look and feel of a brand

Graduated Risk-Based Friction

Preventive protocols evolve as attack patterns change and ensure good customers aren't penalized

Accessibility and Language Support

Arkose Enforce meet Section 508 standards for people of varied abilities across 96 languages

Long-Term Advantage

Fraudsters in the digital economy have accumulated an arsnel of tools and data to attack companies and commit fraud. Arkose Labs safeguards stage of the customer journey with superior risk management. This proprietarry approach provides a long-term advantage by disrupting the fraudsters' business model while delivering a seamless customer experience.

Long-Term Prevention

Strategic setbacks compel bad actors to give up by making fraud and abuse economically irrational

Real-Time Remediation

Combined approach instantly resolves conflicts that exist between user identity and intent

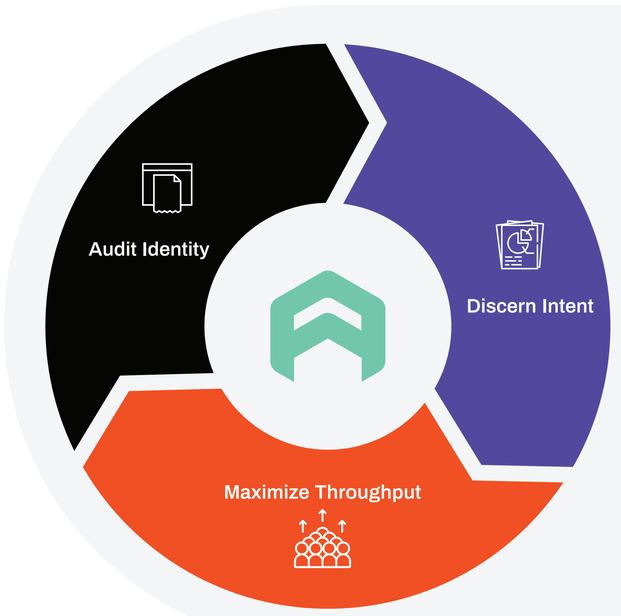
Extended Intelligence

Unique insights neutralize attacks around the world as network effect shares them across the platform

Future-Proofing

Self-optimizing Arkose Detect and ongoing improvements to Arkose Enforce fortify the platform as threats evolve

Combined approach for assurance and growth



Audit Identity
Leverage more reliable data to establish the origin of each transaction

Discern Intent
Validate analytics to evidence the underlying motive of all transactions

Maximize Throughput
Remove unnecessary friction and never block customers

Demonstrated Results

17% ↗
Revenue for a travel company

33% ↗
Genuine user throughput for a tech platform

15x ↘
Fraud reduction for a gaming company

Eliminated spam and bot traffic for a social network

Schedule Demo demo@arkoselabs.com | (800) 604-3319 | www.akoselabs.com