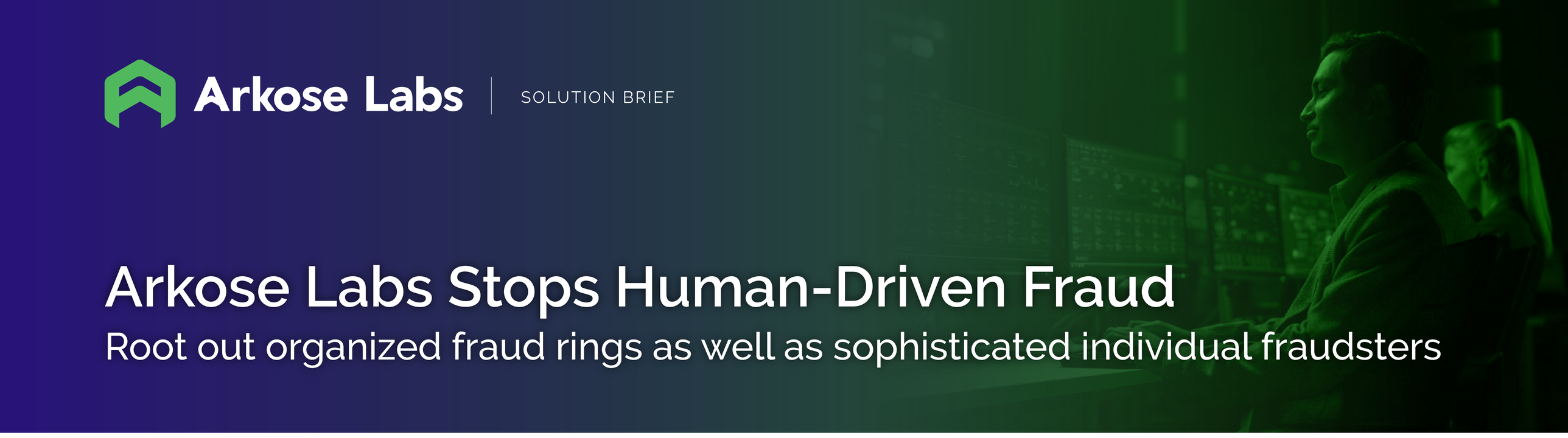
Arkose Labs | SOLUTION BRIEF



Arkose Labs Stops Human-Driven Fraud

Root out organized fraud rings as well as sophisticated individual fraudsters

People Power the Fraud Ecosystem

Fraudsters rely greatly on automation to launch attacks at scale and ensure they hit a wide range of targets. But bots alone do not power the global fraud ecosystem. People are an integral part of many different types of fraud attacks.

Fraudsters often deploy human fraud rings in conjunction with bots, in so-called "cyborg" attacks, where humans step in to circumvent anti-bot defenses. Fraud rings are also used as cheap labor to create fake new accounts at scale, keeping fraudsters' costs low to ensure they make an ROI on attacks.

Humans are indispensable to powering the many different types of fraud that occur around the world today, and this type of fraud is only increasing: Human-driven fraud detected on the Arkose Labs network increased sixfold during the first half of 2021 compared to the previous year.

Protecting Digital Businesses from Human-driven Fraud

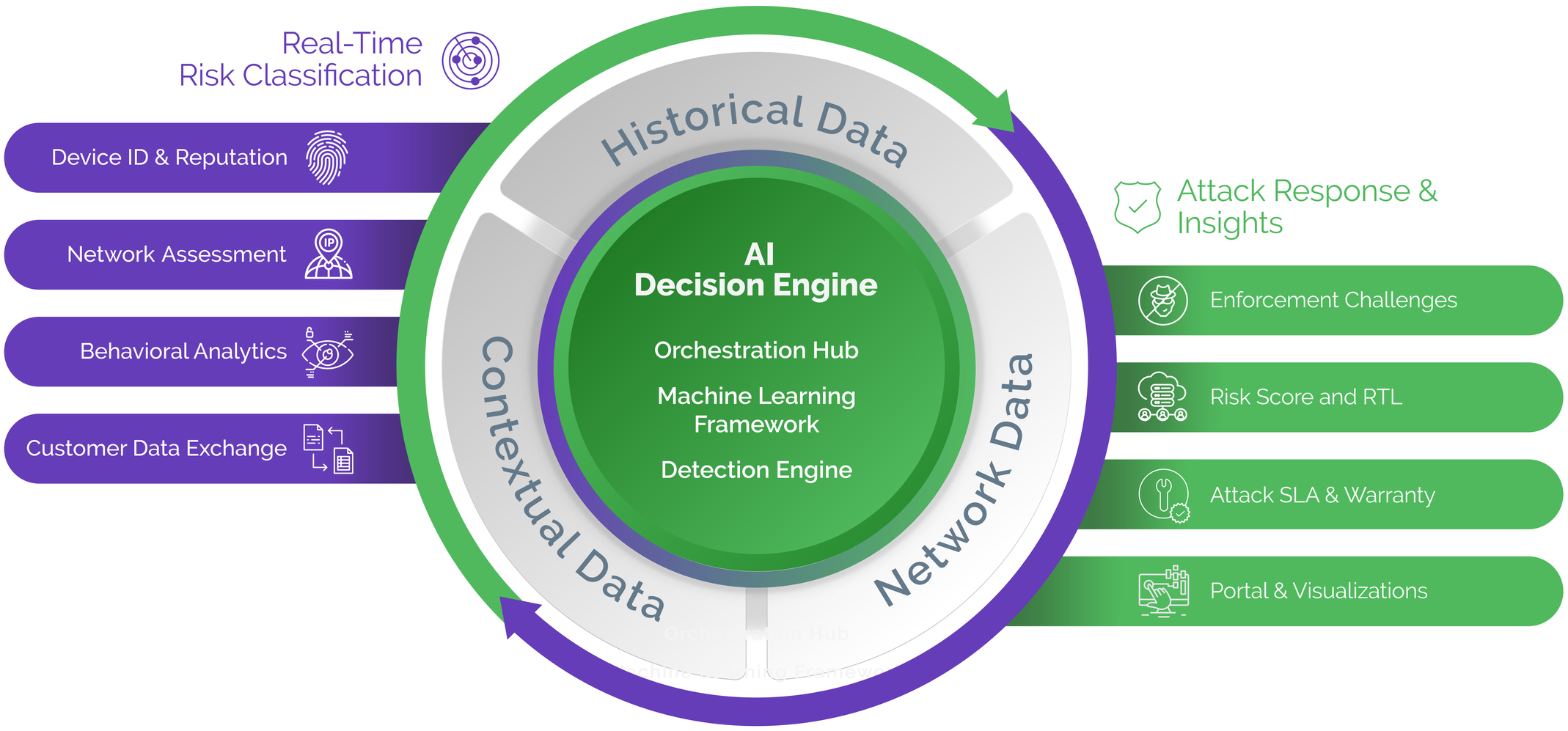
Arkose Labs can help businesses in all industries detect and stop these types of human-driven attacks.

When human fraud traffic is detected, Arkose Enforce works to slow down and frustrate these attackers so that they are compelled to give up attacking. Many of these fraud ring workers get paid to solve anti-automation challenges or per account created, so slowing them down means they are not making money and will instead move on to attack other sites. This is done by serving human fraud traffic with increasingly complex challenges, or challenges designed to time out before they can be completed. It's critical to stop human fraudsters at the digital front door, because they can commit a wide range of downstream attacks.

Arkose Labs stopped 82 million human-driven attacks in Q1 2021 alone and wasted 40 million of fraudster's hours in 2020.

Arkose Labs Fraud Deterrence Platform

Arkose Labs delivers long-term fraud and account security, by undermining the economic drivers behind attacks. Our AI-powered platform defeats coordinated human attacks on the most targeted user touchpoints on websites and apps. Invisible risk assessments allow good users to pass through seamlessly. Malicious human traffic is triaged for active attack response that wastes time and deters future attempts, creating 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 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.

24/7 SOC Support

Our dedicated SOC works with clients to tune the platform as necessary and actively tracks fraud ring operations and known fraud marketplaces.

Arkose Enforce

Arkose Enforce delivers targeted attack response that break the economics of human-driven attacks and makes them non-viable. User interaction data provides immediate insight and truth data on suspected malicious sessions.

Timed Mode

Maliicious humans are fed challenges specifically designed to time out before being completed, which severely hinders fraud ring activity that relies on multiple accounts and devices being used at the same time.

Graduated Friction

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.

Inclusivity & Compliance

Our platform works in more than 100 languages, automatically displaying the language of the browser setting. Challenges are also Section 508-compliant with available audio and keyboard controlled challenges to be inclusive of people with varied abilities.

Custom Challenges

Rather than continually re-using the same challenges, our team of technical artists are continually developing and devising new challenges, meaning fraudsters can't engage in offline puzzle practice

Arkose Global Network

Arkose Labs takes a consortium approach to fraud, leveraging anonymized threat intelligence from over 4.1 billion 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 Advantage

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

Effortless management
Powerful decision engine selects the most effective response strategy to reduce manual reviews

Protection across the customer journey
One flexible solution that protects against different attack vectors and extensive user touchpoints

Early detection
Eliminate losses, reduce costs, and streamline efforts by preventing attacks before they advance in your ecosystem

Privacy friendly
Arkose Lab technology achieves unparalleled accuracy without compromising data protection compliance

Quick results
New customers will see results within days, not weeks or months. Onboarding is quick and seamless.

Arkose in Action

eComm Giant Beats Fake New Accounts

One of the world's largest ecommerce marketplaces was targeted by human fraud farms to set up fake new accounts at scale.

Impact:

- Downstream abuse of fake reviews, selling fake items, and spam
- Existing security measures were damaging good user experience

Results:

- 54% reduction in fake new accounts created
- No damage to good user throughput rates

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
- This would often cause severe cluster failures

Results:

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

Insurer Keeps Fraudsters out of Claims

A consumer electronics insurance firm was facing targeted phishing attacks against its customers by attackers saying they needed certain information about the insurance policy.

Impact:

- User experience was hindered due to frequent attacks
- Fraudsters used customer information to submit fake claims

Results:

- Nearly all phishing attacks stopped
- Almost 6 hours human fraudster's time wasted per day

> "Through data sharing with Arkose, we saw double digit improvement week over week in the number of registrations we were able to identify as fraudulent. They have helped us catch 80% of the fraudsters before they can send out messages to genuine users."
>
> Online Dating Platform

demo@arkoselabs.com
arkoselabs.com

Schedule Demo

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.