Arkose Labs | SOLUTION BRIEF

Arkose Labs For Insurance

Keeping Sensitive Customer Data Safe

Insurance firms store countless records of personally identifiable information. This data is vital for consumers and insurers, but for fraudsters, it represents a gold mine. Fraudsters target insurance firms and their user accounts to gain access to this sensitive data and use it to commit identity theft or further crimes, or re-sell for a profit.

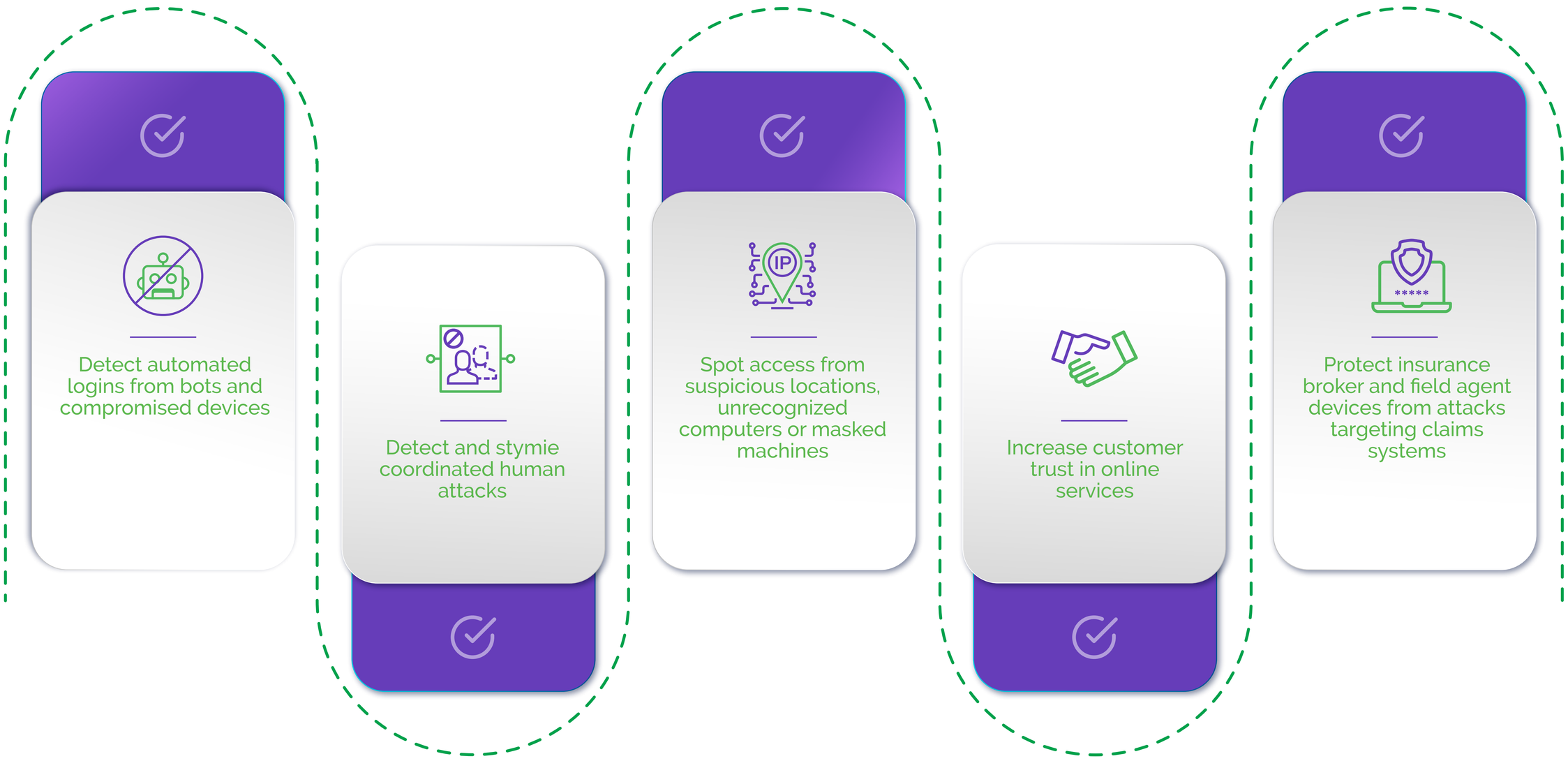
And it's not just insurers directly that are targeted, your partners such as brokers and field agents are in the crosshairs of fraudsters. That's why the entire insurance ecosystem must be protected and all venues to accessing this critical information must be shut off for fraudsters.

Protecting The Insurance Ecosystem

Arkose Labs takes a new approach to fraud prevention, with long-term deterrence by eliminating the ROI behind fraud attacks. Arkose Labs accurately detects even the most sophisticated bots that are used to commit account takeovers and generates real-time challenges that are unsolvable by automation. At the same time, human fraud rings that attack sites are identified and fed increasingly complex challenges so that they give up their effort entirely.

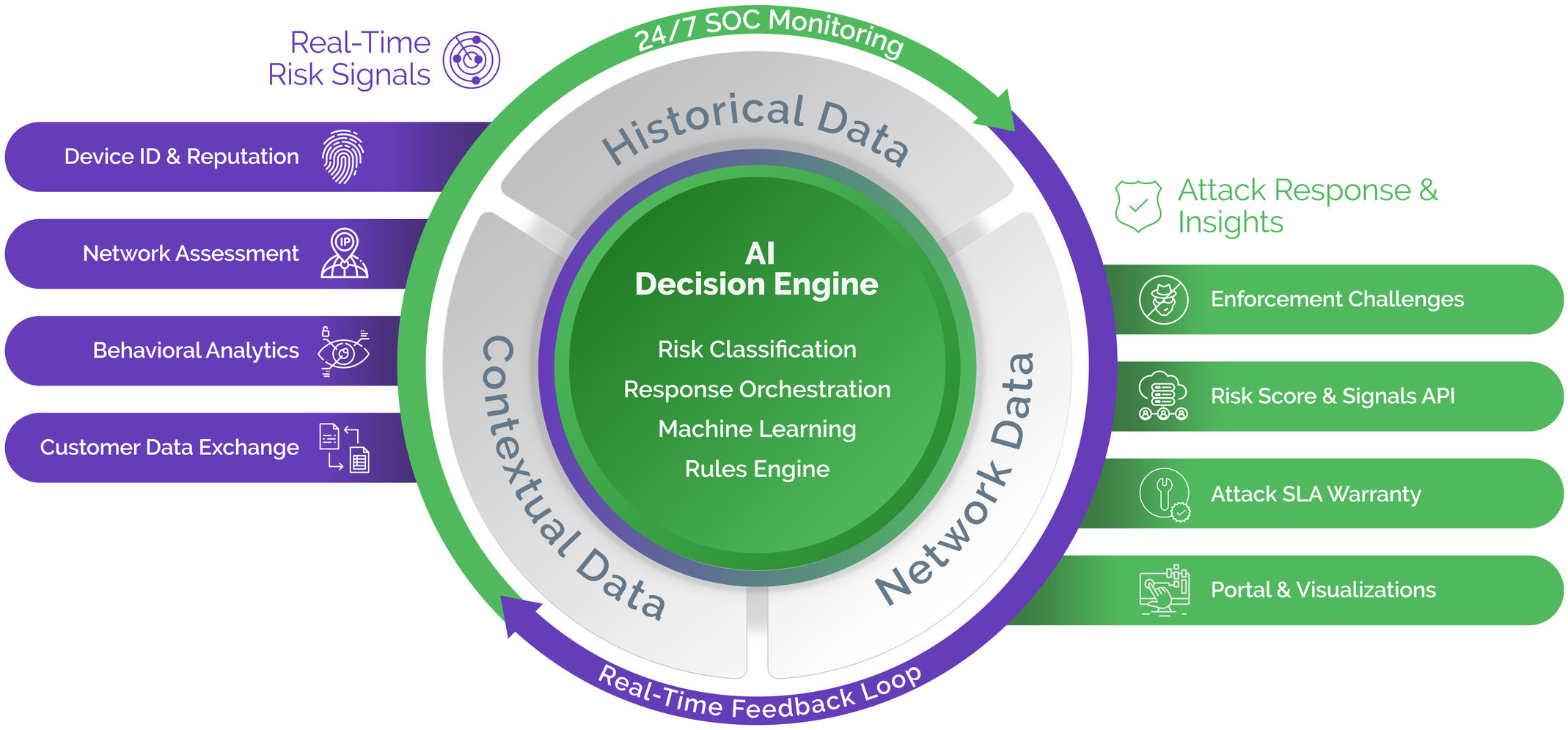
Arkose Labs also stops new account fraud directed at insurance platforms. Fraudsters often use synthetic IDs or other stolen data to submit false claims to insurance companies, looking for big payouts. Whatever avenue fraudsters target, Arkose Labs can help keep you, your partners and customers safe.

How Arkose Labs Protects the Insurance Industry



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 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.

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 and mobile.

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: Attack Response and Deterrence

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.

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

Custom Challenges

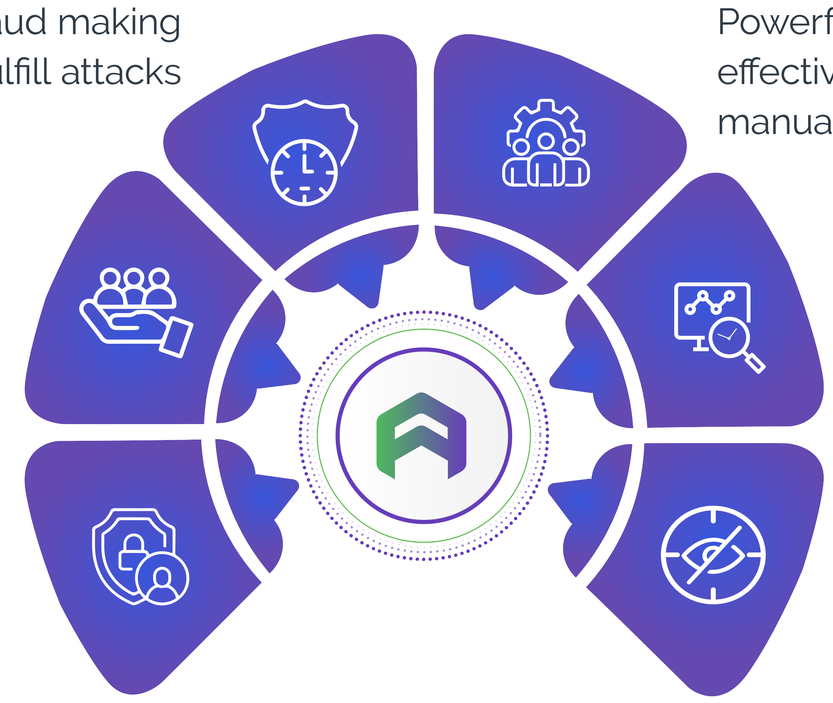
Rather than continually re-using the same challenges, our team of technical artists are continually developing and devising new challenges, meaning fraudsters can't engage in offline puzzle practice

The Arkose Advantage

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

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

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



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

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

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

Arkose in Action

Insurer Keeps Fraudsters Out of Claims

Targeted phishing attacks were carried out against customers by attackers pretending to be the client, saying they needed certain information about the insurance policy.

Impact:

- Fraudsters used stolen credential to submit false claims
- Users experience significantly disrupted, which harmed brand reputation

Results:

- Nearly all phishing attacks stopped after Arkose Labs was implemented
- No negative effect on user experience and significant uptick in customer retention

Dropbox Protects Millions of Accounts With Arkose Labs

Dropbox utilized the Arkose Labs Platform to stop fraudsters looking to abuse the sign-up process and hack into genuine users' accounts

Impact:

- Targeted by account takeover attacks
- Sign-up process abused for account enumeration

Results:

- Greater resilience to account takeover attacks
- Intervention rates for customers slashed by 70%

Outlook.com Stops Fake New Account Creation

Outlook.com was the target of fraudsters looking to create fake accounts at scale to then disseminate spam and malicious content

Impact:

- Fake new accounts created at scale
- Good users were being disrupted

Results:

- 98% reduction in fraud and abuse
- 33% increase in 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.

Email:
demo@arkoselabs.com

Schedule Demo