Arkose Labs

Beyond Digital Identity

The Next Wave of Fraud Detection

Protecting your business in a world where digital identifiers can no longer be trusted.

Introduction: A New Stage in the Post-Breach Era

The explosion of digital commerce has disrupted nearly every industry across the globe. As more and more of our daily lives moves online, however, transactions and digital interactions are exposed to increasingly sophisticated fraud attacks. As a result, many businesses find themselves in a constant fight against evolving fraud and abuse as they try and protect both their consumers and their own profits. In a world where face-to-face interactions have been replaced by device-to-server connections, the concept of identity has changed fundamentally. Identity online is not based on human characteristics or physical identification documents, but purely on data.

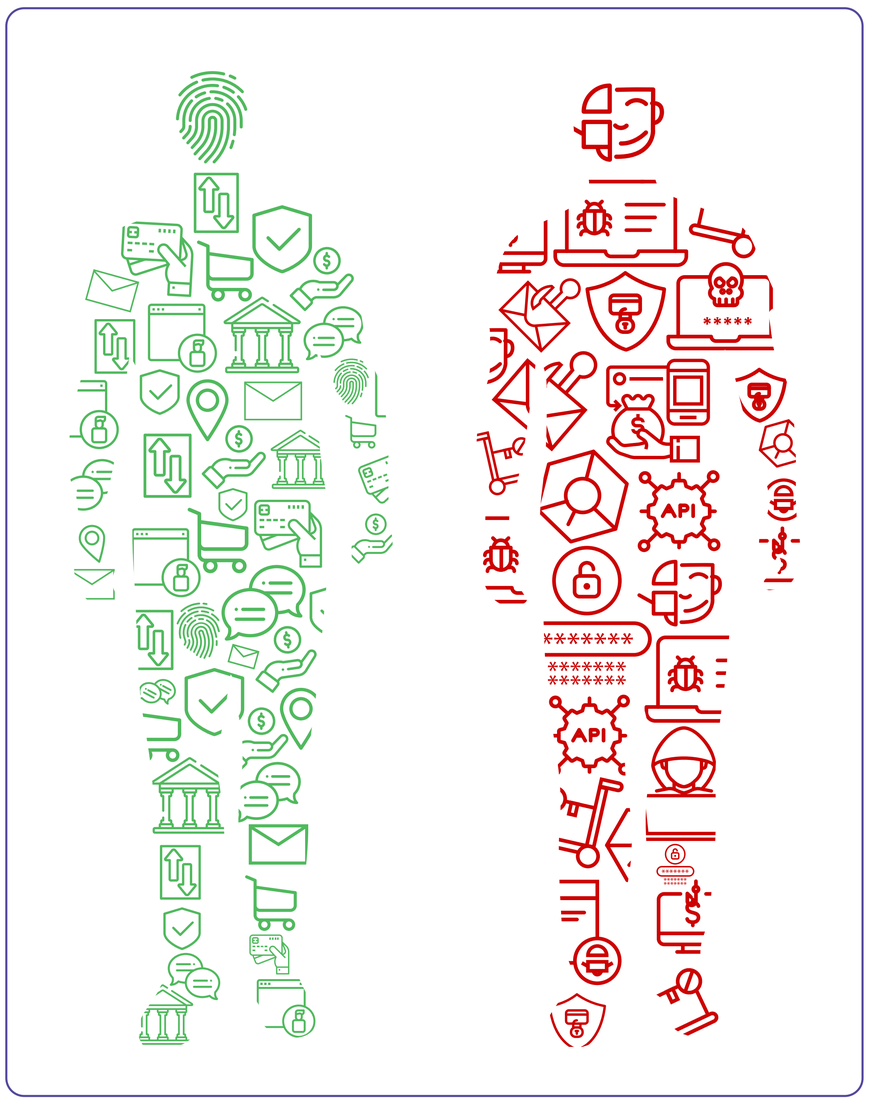
Digital identity intelligence has emerged as a way to harness static and dynamic data in order to differentiate between trusted and fraudulent activity and ensure a smooth user experience for legitimate consumers. Analyzing a series of data points which have been associated to a user over time, such as device characteristics, locations, transaction habits and associated user credentials, provides insight into who is really behind a device or transaction and what the underlying intent is.

However, there is a constant cat and mouse game between fraud prevention teams and cybercriminals, which is undermining how accurately true identity can be determined online. Fraudsters are equipped with new tools and increasingly detailed data insights, and are constantly evolving their techniques as they learn from previous attacks. It has never been easier for fraudsters to masquerade as a trusted digital identity and cloak their true intent.

Recognizing the limitations of traditional, data-driven fraud detection, we must take a fresh look at how to stamp out fraud and abuse, whether it originates from automated attacks, digital sweatshops or more highly-skilled lone fraudsters.

Compromising Digital Identity

Digital identities have been corrupted and attacked en masse by fraudsters. Armed with accurate knowledge of the fraud detection parameters used to detect online abuse, fraudsters are able to use their own defenses against the businesses they attack in order to masquerade convincingly as trusted consumers.



Identity Credentials

Major data breaches have been making the headlines for some years now, however, the gravity of the data breach problem has now entered a distinct new stage. 2019 has been the most prolific on record, and the variety of data now available to fraudsters has reached new heights.

Wholesale identity farms are in operation, systematically checking & verifying stolen credentials and selling them on the dark web. Synthetic identities are stitched together using a mix of legitimate stolen data & fabricated information. These can sometimes be even more powerful for a fraudster, as there is not always an individual flagging misuse, providing a longer window of opportunity to monetize that identity data.

Device Intelligence

The devices consumers transact on have been long used as a stand-in for identity in the digital world. Activity from a device previously associated with trusted user activity is often automatically given the green light, without further detailed inspection.

However, in the new wave of data now available to fraudsters, they are able to purchase cloned fingerprints of trusted devices. Alternatively, they leverage tools that randomize device characteristics in order to appear as a new device. Organizations that rely heavily on historical device intelligence to assess whether a user is legitimate or not will often err on the side of trusting the consumer when there is a 'new' device, to avoid blocking legitimate customer transactions or logins.

IP Address and Location

There has been a long-running arms race between location spoofing and proxy piercing technologies. However, to complicate matters, fraudsters are now leveraging tools that let them appear from a trusted residential IP address connected to a user. Alternatively, they will spoof their IP addresses to appear from a benign source. With location spoofing tools becoming increasingly sophisticated, fraudsters can appear to be transacting from a known or trusted location, undermining a crucial component of digital identity assessments.

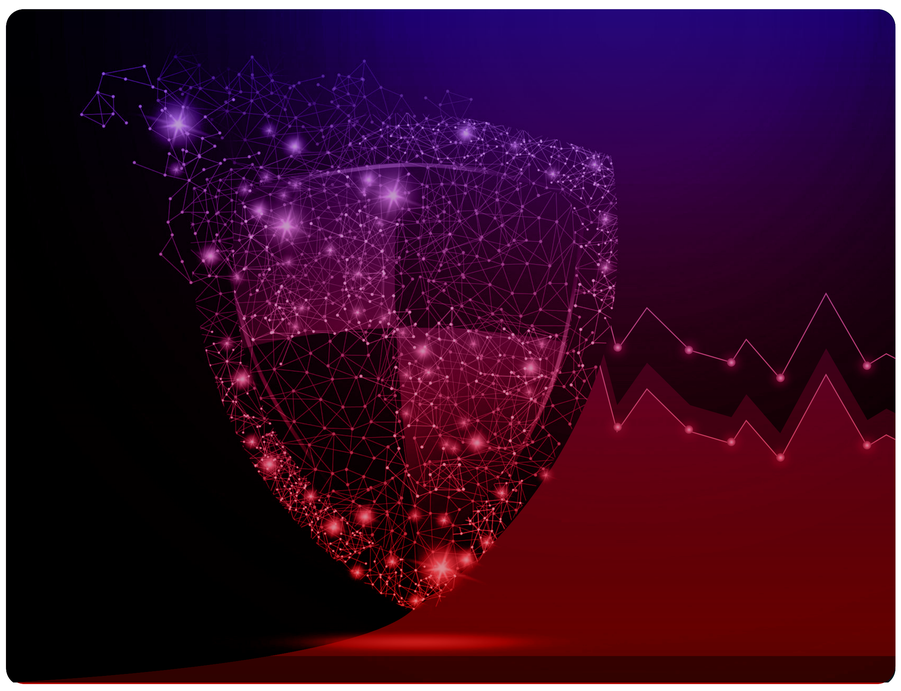
Behavior Analytics

Fraudsters have learnt how to fool behavioral biometrics solutions using sophisticated bots that can mimic human activity. Additionally, targeted attacks by lone fraudsters are supported by previous account takeover attacks, which provide insight into specific user behavior. Gaining insight into the transactional habits and behavioral patterns of an individual provides a more complete picture of a targeted digital identity, and this is used to circumvent anti-fraud controls.

The Impact on Fraud Decisioning

Data-driven decision engines are geared towards extremes, looking for users that display clear 'trust' or 'mistrust' signals. They, therefore, struggle with the new reality in fraud, where digital identities have been corrupted and intent faked.

There is a growing gray area due to unpredictable behavior from good customers and sophisticated spoofing and cloaking techniques from fraudsters leveraging stolen personal data. If one factor is off for a good user, for any number of legitimate reasons, then it can throw off the whole fraud prevention model.



This uncertainty leads to false positives which block legitimate transactions; false negatives where fraudsters successfully execute attacks; or increased levels of friction and manual review which slows down transactions and alienates customers. These ultimately lead to lost revenue, increased fraud losses and spiralling operational costs.

A New Paradigm: Beyond Digital Identity

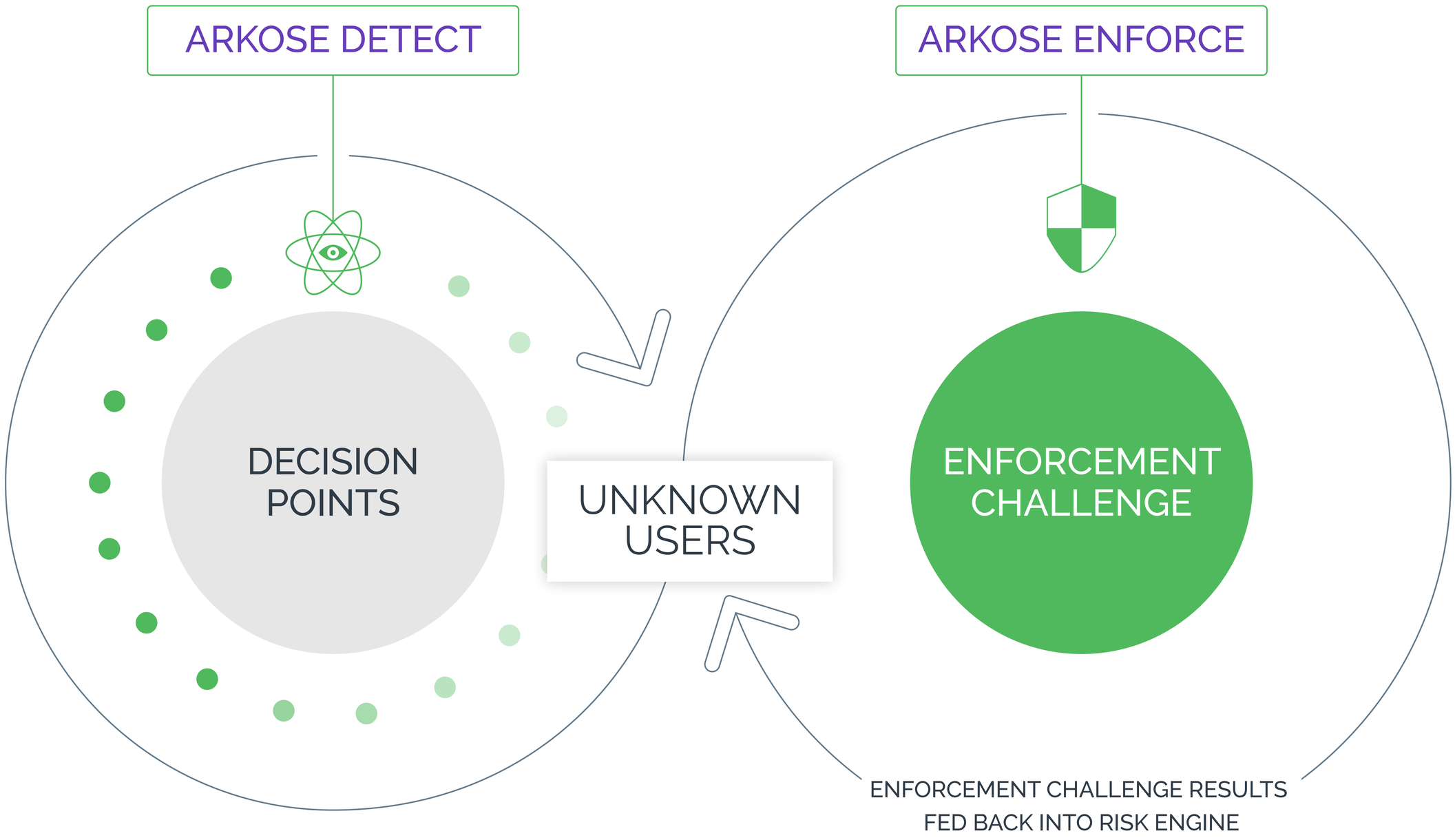
Rather than businesses playing a constant cat and mouse game with fraudsters, they need a long-term approach to disrupt fraud and put a stop to large-scale attacks. Accurate fraud decisioning must account for the fact that digital identifiers and device information have been hacked and cannot easily be trusted. The next level of intelligence assesses not only static device information, but looks at how the device is interacting with the network to see if fraudsters are using tools to subvert the systems.

A more robust and accurate approach to fraud detection in this environment is one that combines risk-based decisioning with intelligent step-up to clarify whether or not a good customer's digital footprint has been corrupted by fraudsters.

Arkose Labs provides a risk engine that looks for the most subtle signs of fraud, in the knowledge that some of the big ticket items used in accepting transactions, such as a known device, are not always legitimate. Traffic is then triaged according to its risk profile and suspicious traffic is presented with targeted authentication challenges. The Arkose Labs platform acts as an intermediary platform, shifting the attack surface and taking control away from the attackers. Detailed risk profiling means when step up authentication is required, enforcement challenges are targeted towards suspected fraud types, and tailored towards bots, digital sweatshops or lone fraudsters.

The Arkose Labs Approach

Arkose Detect, an advanced risk engine, does not rely on extremes in data but analyzes in depth and breadth across all parameters. This integrates seamlessly with Arkose Enforce, which provides intelligent step-up authentication tailored towards the risk profile. Arkose Detect and Arkose Enforce work seamlessly together and inform one another for improved future prediction and identification of malicious traffic. Deploying machine learning further sharpens anomaly detection & trains the platform in real-time, with the challenge as the feedback loop.



Key Benefits: The Arkose Labs Fraud and Abuse Platform

Constant feedback loop between risk engine and enforcement makes Arkose Labs the fastest learning fraud platform on the market, specifically geared for constant self-improvement.

Shifts the attack surface from the business to Arkose Labs' independent platform. As a result, fraudsters are no longer attacking their targeted customer touch point but are diverted to intelligent step-up that saps their resources.

Deep analytics to detect sophisticated fraudsters, that factors in the new reality where fraudsters have corrupted digital identities at scale.

Makes attacks more difficult and costly, which disrupts the fraudsters' economic incentive and breaks their business model.

Longer-term solution that stops the cat and mouse game that fraudsters play with businesses.

Delivering Maximum Defense and Greatest User Experience

Arkose Detect and Arkose Enforce work together to determine the best authentication workflow and protect against evolving threat patterns. Authentication that is tailored to the risk profile provides the optimal balance between greatest user experience and greatest security.

Legitimate Consumers

- No challenge for most true users, providing a friction-free experience.
- Humans are never blocked, but when step-up authentication is required this provides the user with an opportunity to prove she is legitimate.
- Challenges are easy and fun to complete, with no negative impact on user experience.

Bot and Automated Attacks

- Targeted step-up challenges root out 100% of automated attacks.
- The Arkose Labs Acid Test introduces uncharacteristic visual data into the challenge–response mechanism, causing automated processes to spontaneously fail.
- Constantly evolving the type of challenge presented prevents fraudsters from scripting past this defense to circumvent at scale.

Digital Sweatshops

- Sweatshop activity is identified using sophisticated profiling and velocity assessments.
- Increasingly complex challenges are presented which waste fraudsters' time and resources, compelling them to abandon attacks.

Lone Fraudsters

- Independent identity verification shifts the attack surface away from the targeted website or app, which the fraudster has had practice attacking.
- The context of the transaction is important in differentiating between a trusted customer and a skilled lone fraudster. Lone actors will concentrate on high-monetization transactions, otherwise they would not get sufficient return on investment.
- Bug bounty program uses ethical hackers to test the platform against skilled lone actors.

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, 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.

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Address:

USA • 250 Montgomery St, Fl 10, San Francisco, CA. 94104

Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006

Schedule Demo