Arkose Labs

EBOOK: BALANCING USER EXPERIENCE WITH FRAUD MANAGEMENT

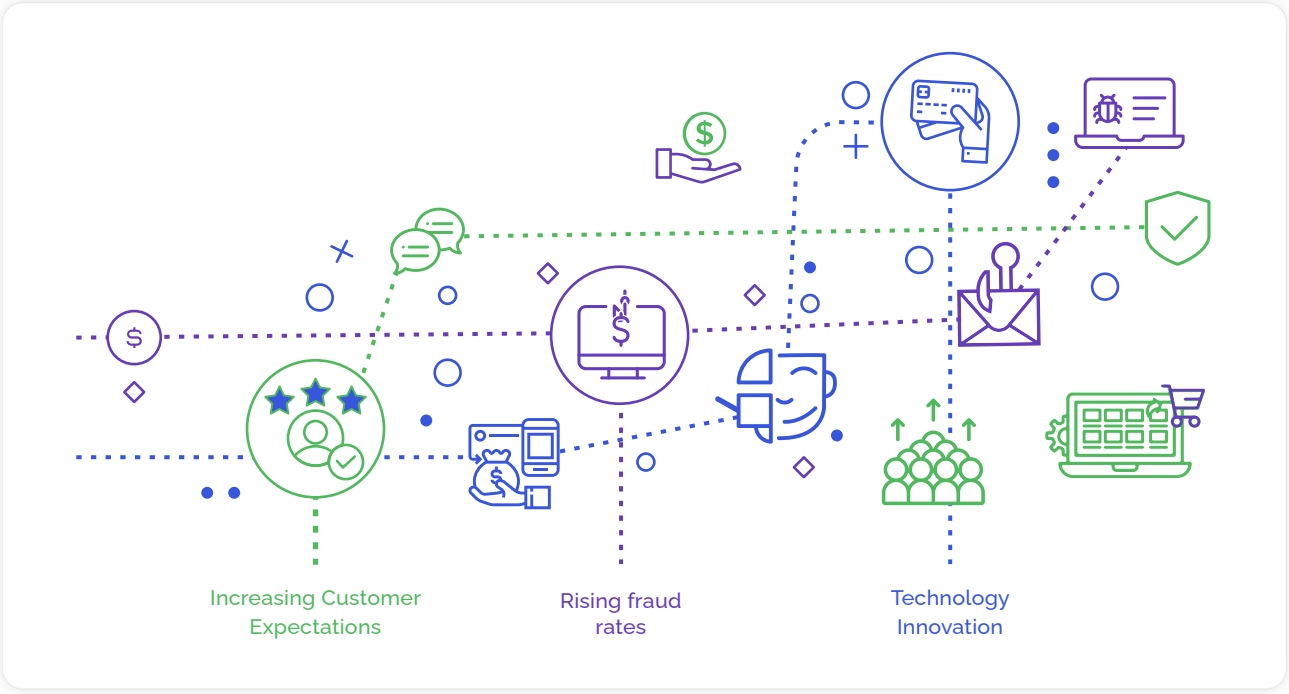
WEB TRAFFIC: HOW TO BALANCE THE GOOD, THE BAD, AND THE SUSPICIOUS

EBOOK

INTRODUCTION

The digital world has created many new opportunities for fraudsters. Attackers use stolen data harvested from large-scale data breaches to launch an array of attacks including fake account registrations, account takeovers, and fraudulent payments using stolen credit card details. As data breaches continue to happen with greater frequency, fraudsters will have no shortage of stolen data to work with.

Digital businesses, on the other hand, find themselves caught between the competing forces of rising fraud levels and heightened customer expectations. Modern consumers want security, however, they show little tolerance for any delays or barriers in their online shopping experience.



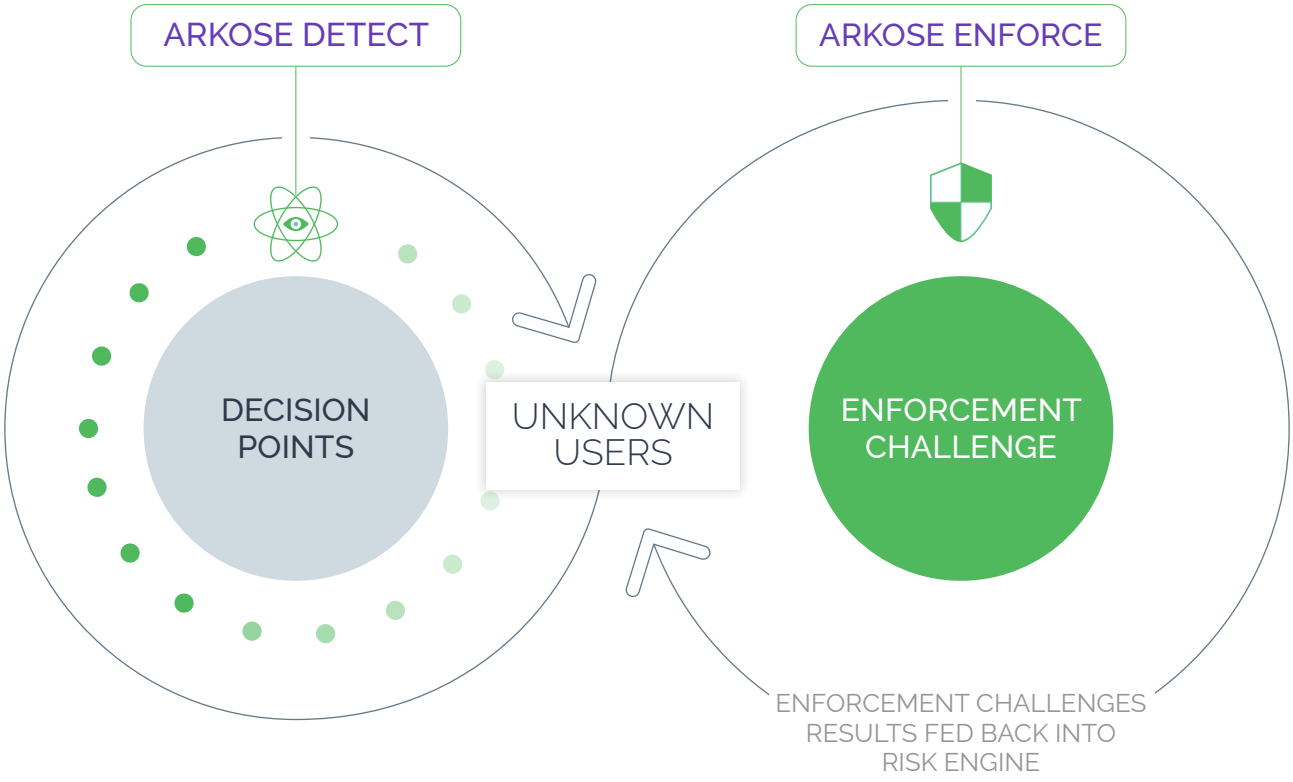
As digital businesses confront the challenge of increasingly sophisticated fraud and the need to meet higher customer expectations, it is essential to evaluate the role of friction in achieving the perfect balance between user experience and security online. Arkose Labs Fraud and Abuse Prevention Platform provides a powerful solution that delivers a great customer experience and throughput while making attacks unprofitable for fraudsters, resulting in considerable cost savings for the business and an improved return on investment.

FRAUD AND ABUSE PREVENTION PLATFORM

The Arkose Labs Fraud and Abuse Prevention Platform combines real-time intelligence, rich analytics, and sophisticated step-up challenges to progressively diminish the profitability of attacks while adapting to evolving attack patterns. Our MatchKey challenges provide a unique user experience, performance improvements, and powerful styling features.

Arkose Detect analyzes data from user sessions in real-time to help recognize the context, behavior, and past reputation of every request and assigns a risk score. Depending on the severity of the score, Arkose Enforce--a challenge-response mechanism--presents every user with an opportunity to prove authenticity. While genuine users can easily clear the challenges, suspicious users and probable fraudsters, looking to clear the challenges at scale, face resistance.

By implementing a system of suspicious traffic management that presents incrementally complex challenges that demand time and extra resources to complete, organizations can save costs and achieve better ROI. This system permanently disrupts the economic viability of organized attacks and breaks the fraud model to stop both human and bot-driven attacks, making it an invaluable tool for protecting businesses.



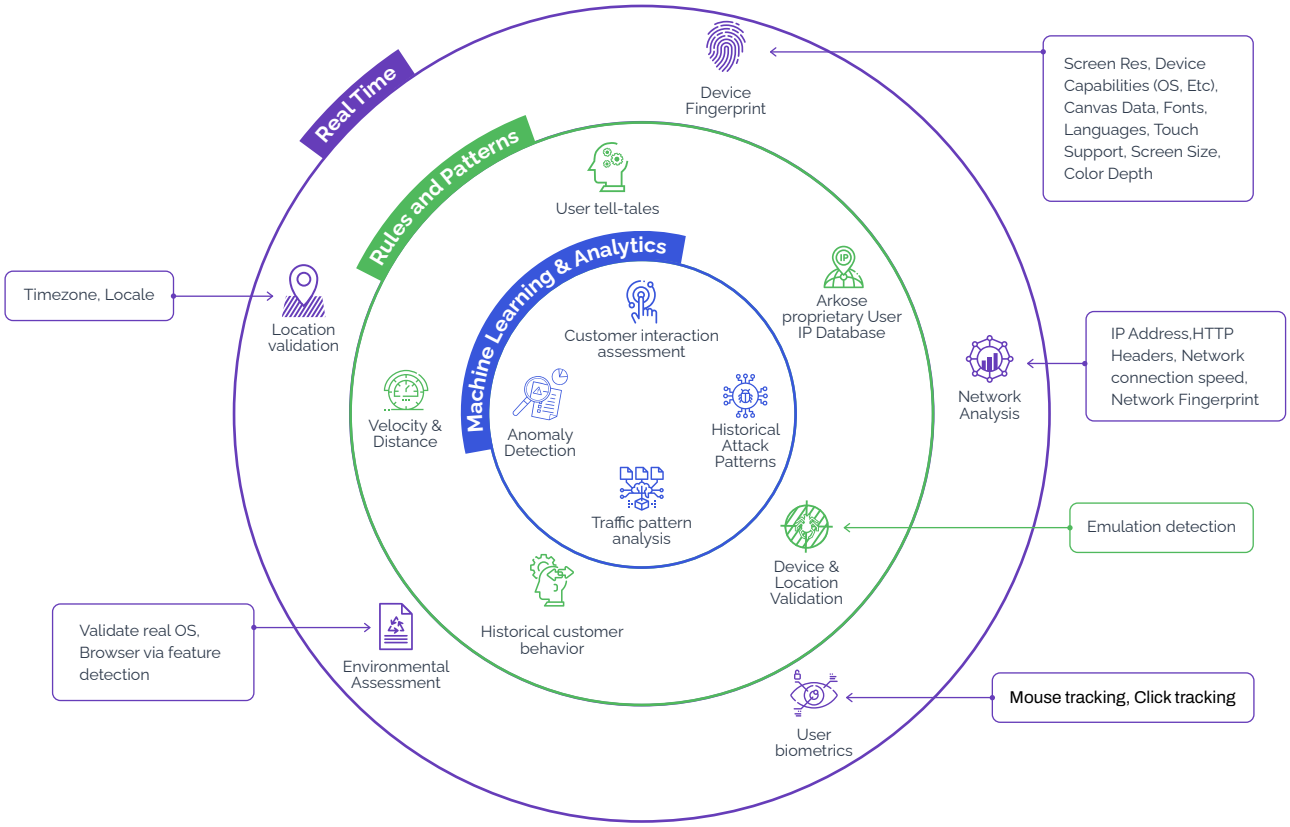
ARKOSE DETECT

Arkose Detect is a dynamic risk engine that analyzes data from user sessions and their interactions with technology. Combining this data with behavioral patterns, Arkose Detect accurately uncovers the underlying intent of the user, which informs Arkose Enforce.

Some key features include:

- **Deep device and network forensics:** Gain 360-degree insight into a user's reputational integrity and assign an appropriate risk profile. This includes device fingerprinting and validation to understand the characteristics and assess the validity of the device.
- **Continuous intelligence:** Combine digital intelligence with behavioral patterns that help discover the underlying intent of a user and segregate users into smaller groups with distinct motivations.
- **Location assessment:** Identify when fraudsters try to spoof their location. Increase suspicion for the levels of activity that are disproportionate to the authentic traffic from that location.
- **Abnormality detection:** Analyze the network traffic patterns in realtime to determine behavior patterns across cohorts.
- **Behavior biometrics:** Analyze user interactions with their devices to identify anomalies and automation.
- **Embedded machine learning:** Detect malicious activity displaying similar characteristics using machine learning. This enables rapid detection and protection against evolving attack patterns across the network.
- **Historical attack pattern calibration:** Shift the attack surface away from the business as Arkose Detect correlates attack patterns across use cases and industries to understand how they are orchestrated. This network intelligence provides valuable insights in detecting anomalous behavior and patterns.
- **Adaptability:** The data from user sessions, as well as the results from Arkose Enforce, is fed back into Arkose Detect to improve future predictions and help adapt to the evolving attack types.
- **Dynamic identifiers:** We find and classify attackers by identifying telltale signs in their interaction patterns, fingerprints, and other signals. As the attacker changes these telltales, our system adapts to keep tracking them.
- **Dashboard and visualization:** An intuitive dashboard uses visualization and data stitching to deliver end-to-end insights across the customer journey. This unifies user data with real-time user behavior and metadata.

Arkose Detect Overview



ARKOSE ENFORCE

Arkose Enforce delivers adaptive enforcement MatchKey challenges that accurately distinguish between authentic users, malicious humans, and bots, thereby protecting against online abuse and fraud. The challenges gradually increase in difficulty depending on the associated risk of the user. This increases the time required for fraudsters and wastes their resources when trying to clear challenges at scale. Since increasing costs diminish the profitability of the attacks, fraudsters are compelled to stop.

Some of the challenge types include:

Welcome to the Internet: An introductory challenge to assess the legitimacy of a new user the first time they are seen on the Arkose Labs network.

Basic bot challenge: Identifies basic automated attacks and presents challenges that bots cannot pass to eliminate this traffic.

Acid test: Distinguishes between a trained bot and a human with a test that uses new images and puzzle types which cause all automated processes to instantly fail.

Trained bot challenge: Presented to traffic which fails the acid test. Arkose Labs then presents a more complex challenge to root out sophisticated automated attacks.

Sweatshop challenge: Presented to traffic which passes the acid test, such as traffic from a click farm. Malicious humans are often distinguished from authentic humans through activity much slower or faster than typical. This challenge deliberately wastes the time and resources of the sweatshop, making it unprofitable.

Proof of work: Invisible to standard users, these forms of tests are used to prove the end-request device has certain capabilities, for example, the ability to execute Javascript or log cookies.

Proof of activity: These challenges are a more advanced form of proof of work, in that not only do you need device capabilities, but you must do something. They are designed to be incredibly simple for regular users and utilized primarily in low-risk scenarios where a user might pass a rate limit threshold as an example.

Key features of Arkose Enforce include:

- **Bespoke and brand-integrated:** Arkose Enforce challenges are created using brand elements that blend with the website or app. This prevents disruption to the user interface and helps deliver a seamless user experience.

- **Self-optimized step-up:** Using real-time insights from Arkose Detect and combining it with the risk profile of the user, the dynamic prevention protocols automatically enforce when necessary. This wastes fraudsters' resources and reduces the return on investment.

- **Breaks the fraud business model:** To bypass the Arkose Enforce challenges at scale, fraudsters must spend more time and invest in extra resources. This makes them financially non-viable.

- **Adaptive:** Regular updates and releases based on the ongoing Arkose Labs research and development help Arkose Enforce challenges to evolve with the changing attack techniques.

- **Accessible:** Arkose Enforce challenges are Section-508-compliant which helps ensure people of varied abilities across 100 languages can respond.

ARKOSE ENFORCE DESIGN & TEST PHILOSOPHY

Arkose Enforce is designed with the customers in mind. While Arkose Detect ensures that the vast majority of authentic users will never see an enforcement challenge at all, Arkose Enforce ensures the fraud model is undermined. The purpose is to make any "false positives" face as little friction as possible.

Where it Began: The foundation of the enforcement challenge lies in the video game design techniques, primarily driven by over 25 years of professional game development experience of the company's co-founder & product head. The development of new puzzle types is done in phases: ideation, design, prototyping, and testing. This is an iterative process, and even existing puzzles are continuously re-tested and improved over time.

1. **Ideation:** A new idea can come from anywhere - from the product team, or anyone else within the company leveraging a diverse cultural and professional background.

2. **Design:** The most promising ideas are fleshed out by the team of security artists. Their primary focus being human comprehension with resistance to automation, a secondary consideration at this stage.

3. **Prototyping:** An initial version of the new puzzle is turned into a static, then fully functional prototype. This prototype is used for internal user testing, with the company's diversity helping identify any cultural stumbling blocks early on.

4. **In-Person Testing:** A refined version of the prototype is now tested outside the company by asking the test subjects to voice their thoughts as they navigate through the puzzle. This helps the teams identify any user stumbling blocks and misunderstandings.

5. **Online Testing:** A successful prototype testing leads to a live production A/B test in very low-volume on selected customers. The "A" case is a well-established easy-to-solve puzzle, and the "B" case is the new puzzle to be tested. This provides detailed analytics and valuable insights into the performance of the new puzzle, as compared to existing puzzle baselines. While the goal is to test insights from just a few thousand sessions, the product team watches these tests carefully and stops the test if the results on an enterprise customer ever look poor.

6. **Machine Learning vulnerability analysis:** The product team then uses machine learning (ML) tools to see how much expert work is required to make a viable solver for the puzzle. These tools have been submitted to the company's whitehat bug bounty program. The puzzle can be adjusted to make it harder for ML tools to automate while preserving the human completion rate.

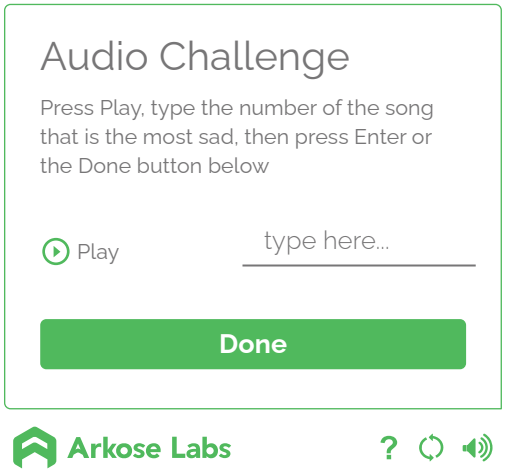
7. **Iterations:** Based on the results of the live production tests, the puzzle is further refined and re-tested to increase the human completion rate, as well as to harden the puzzle against automated attacks.

8. **Sweatshopping:** Some puzzles are designed to absorb as much human time as possible, while still being solvable. These puzzles are issued to sweatshops or organized fraud rings. The product team carefully measures the time it takes to complete the puzzle and adjusts it to maximize this time.

9. **Production vigilance:** Our Customer Success team constantly monitors performance of all enforcement challenges given to legitimate users to assure nothing goes wrong.

For audio challenges, the services of a professional accessibility lab are employed to conduct comprehensive in-person user testing with vision-impaired users. These tests focus both on the accessibility aspect of the solution, as well as on the comprehensibility of the audio puzzles.

This entire process revolves around the user experience and human completion rates first and foremost. The product philosophy is based on providing a simple and low friction experience for authentic users with additional techniques being layered on to make the same puzzle secure against automated attacks as well. The benchmark first-time completion rate for authentic users has to be above 95% and most of the puzzles attain 98% or higher. Even if an authentic user falls into the tiny percentage that does not complete an enforcement challenge session, it does not mean the user is lost forever. We find that good users will often come back to the page to try again and succeed. That's good news for your business.

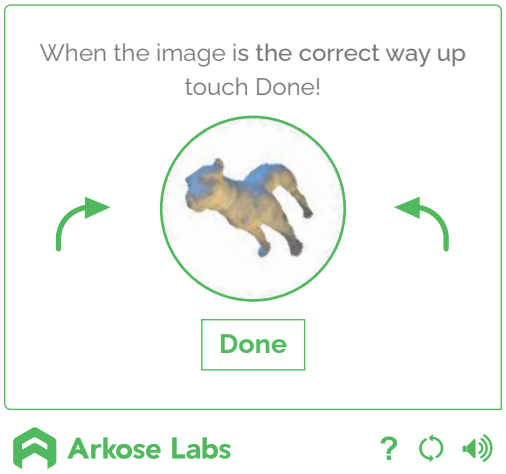


ARKOSE ENFORCE USER METRICS

Below are the user metrics for Arkose Enforce:

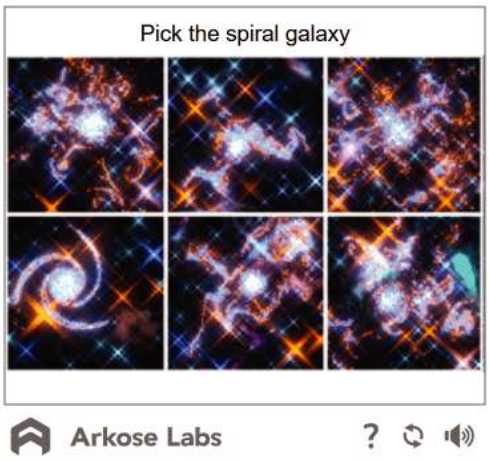
Roll the Ball - with a single animal:

- Average completion rate: 97.4%
  - These users solve the puzzle correctly (with or without failed attempts along the way) and are free to continue along the user flow.
  - Completion rate up to 99% on some sites.
  - About 6.3% of users submit an incorrect answer to the puzzle and are prompted to try again. Nearly all of them do try again and solve it correctly on the second attempt.



Rotation Puzzle - with unusual and partly obscured animals:

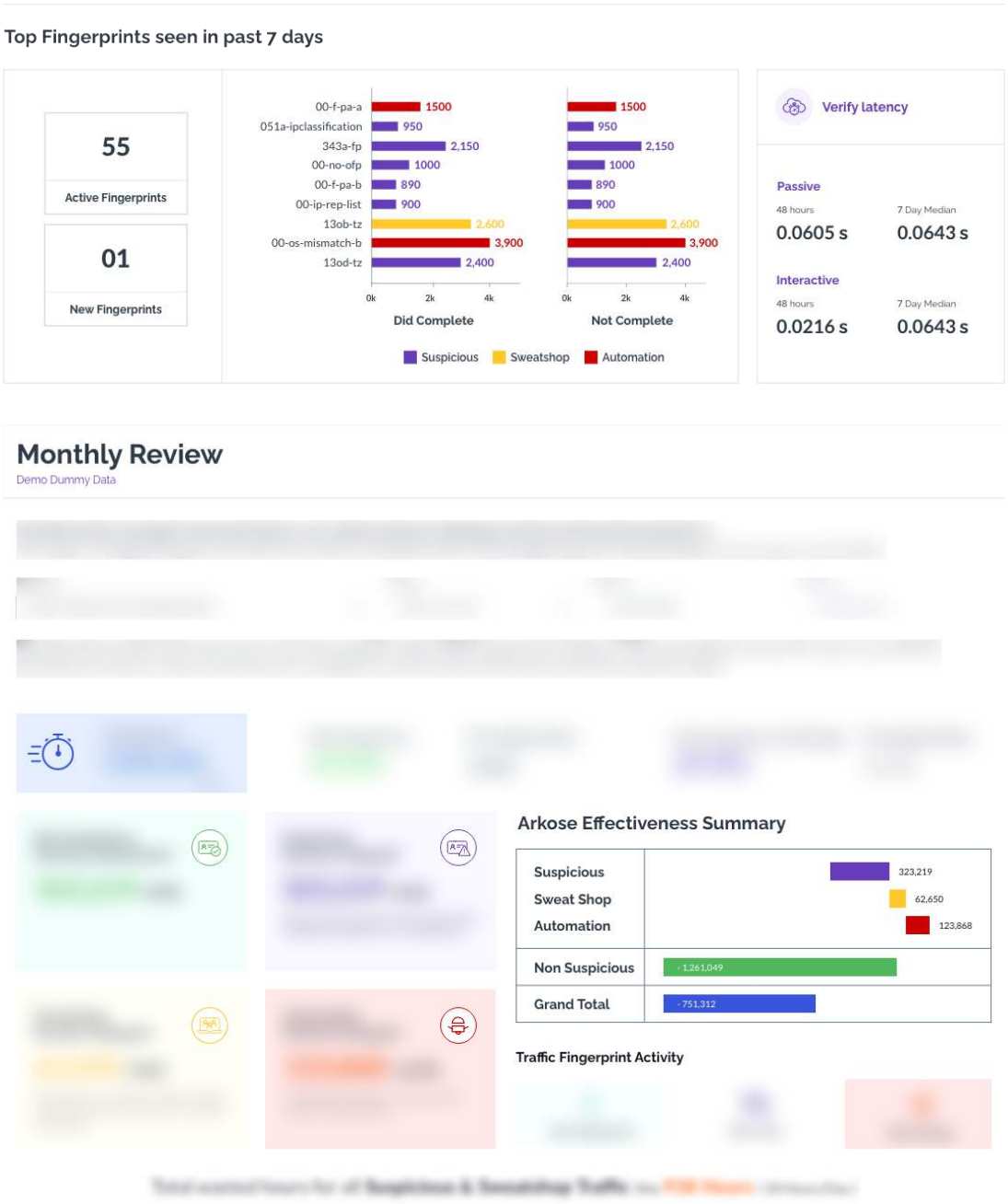
This challenge is not used on authentic traffic but in test scenarios. This has a completion rate of up to 98% for this game type.



Pick a tile :

There are several variants in this format, "Pick the spiral galaxy" is one example. The current tests indicate excellent completion rates. Both completion rates and fail rates are continually improved.

DASHBOARD & ANALYTICS AROUND USER METRICS



DEMONSTRATED RESULTS

Microsoft: 33% improvement in preferred customer throughput with 7.5X increased fraud detection.

Travel Portal: 96% reduction in fraud and elimination of BOT activity with no impact on good customer throughput.

Social Media Platform: 19% increase in customer engagement with a 22% reduction in scraping.

Social Streaming Platform: 8.6% reduction in downstream customer banning while improving good customer experience.

FinTech Platform: Increased good customer throughput by 10% while reducing the use of stolen and/or fake user details by fraudsters for new account registration and account takeover attempts.

Roblox: In an A/B test against reCAPTCHA V2 ("Are you a human checkbox"), found that Arkose Labs had a 15% improvement on revenue, whilst dramatically reducing abusive traffic.

CONCLUSION: STOP TREATING YOUR CUSTOMERS LIKE CRIMINALS

Many fraud prevention departments have bigger budgets than ever before, but are barely keeping the rising fraud levels, or the cost of fraud management, at bay. And with consumers expecting a seamless, friction-free experience, digital businesses have become a prime target for large scale identity and payment fraud.

Businesses, in turn, have struggled toeing the fine line between enabling a great user experience while still being vigilant in fighting fraud. But rather than completely shying away from introducing friction into the customer journey, it is time to rethink how this can be leveraged as a positive component that supports risk-based decisioning in a complex threat landscape.

Arkose Labs offers the optimal balance between user experience and protection against fraud and abuse in all its forms. Sophisticated analysis from Arkose Detect ensures that the vast majority of good users proceed unchallenged, but the nature of the challenges presented by Arkose Enforce makes it simple for legitimate users to complete these should they need to.

This targeted friction is highly effective at undercutting the financial incentives behind fraud, helping businesses across industries to save time, money, and resources while eliminating automated attacks and sapping the resources of large-scale, human-driven attacks. As a result of this fundamental shift in fraud prevention, businesses can expect to see improved cost savings and better return on investment (ROI). There is also no negative impact on good user throughput.

Arkose Labs

Arkose Labs deters fraud while offering a seamless good user experience. 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 motivation behind attacks, providing long-term protection while improving good customer throughput and overall ROI for the business.

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