A NEW APPROACH TO FRAUD PREVENTION

EBOOK

BEYOND THE POST-BREACH ERA

While investment in fraud prevention solutions among businesses has never been higher, the volume and severity of fraud continues to rise - with far reaching impacts on our society. The major data breaches which feed large-scale fraud attacks have been making the headlines for some years now, however, we have now entered a new stage in the post-breach era. Digital identities have been corrupted and attacked en masse by fraudsters with easy access to vast swathes of personal information, using sophisticated tools that simplify the monetization of stolen data.

Businesses need to update their fraud prevention strategy in the face of this new reality. For many years now, there has been a focus on mitigation strategies that attempt to address the rising tide of fraud, without truly getting to the core of the issue. Widespread tolerance for existing fraud levels, with the attitude that it is a 'cost of doing business', actively feeds the vicious cycle of successful cybercrime and provides the financial incentive for fraudsters worldwide to continue and expand their operations. It also gives them an opportunity to learn from past attempts and replicate attacks elsewhere.

THE CONNECTED ECOSYSTEM

It is said that cybercrime is now more profitable than all of the world's drug trade combined, with annual losses predicted to reach $6 billion by 2021. Losses at this scale could not be achieved by lone fraudsters working in silos. A complex ecosystem that has sprung up to support the business of fraud is multi-faceted, with 'services' such as identity farms, arms dealers, sweatshops and money mules, making it possible for large-scale, organized fraud to exist. These are accessed through the Dark Web, alongside forums which share the latest and greatest tools and techniques that are working against current business preventions.

Fraudsters are able to keep costs low by casting their nets globally and taking advantage of regional economic disparities to access cheap resources. While cybercriminals' costs are able to consistently drive profits operating this way, businesses are experiencing ever-expanding demands on their budgets. For a sustained fight against cybercrime to be successful long-term, we need to focus on eliminating the economic advantage of fraudsters versus the businesses they target.

> We're extremely pleased with Arkose Labs and their ability to solve a very expensive problem for us. I'd definitely recommend Arkose Labs for online abuse, fraud, or other damaging automated attacks
>
> —Airline

THE CHANGING FACE OF FRAUD

The majority of fraud attacks detected on the Arkose Labs network continue to be automated. However, there is a marked trend of increasing human-driven attacks, and an evolution in the automated tools that are used to circumvent anti-fraud controls.

Bots and Automated Attacks:

Bots have long been used to attack businesses, using automated scripts aimed at credential testing and account takeover attacks. Businesses have put protections in place that make it simple to detect the most basic of these. However, trained bots have evolved to mimic customer behavior and there has been a rise in single request attacks which use technology to obfuscate or spoof IP addresses and any other identifying characteristics that are used for fraud detection.

Digital Sweatshops:

The global cybercrime ecosystem provides access to click farms or sweatshops, where large teams of lower-skilled workers are made available for hire. These help launch or assist attacks which require some human interaction or more nuanced tactics than large-scale bot attacks. While this drives the costs up for perpetrators, they can be very effective in bypassing controls aimed at detecting automated attacks and perpetrating fraud that requires humans, for example creating a fake listing on an online marketplace.

Targeted Human Driven Fraud:

As anti-fraud technologies improve at detecting automated attacks, and fraudsters get more inventive at monetizing customer interactions, there is a more significant role to be played by highly skilled fraudsters who launch targeted attacks. Because of the economics involved, this is only worthwhile when there is a high potential for monetization - for example, attacks on financial institutions or targeted attacks on in-game currencies and assets within online gaming.

> It makes us feel good that we are providing a streamlined experience that works well with our target audience.
>
> —Gaming Company

IMPACT OF RISING LEVELS OF FRAUD

The digital economy has prospered on the back of free and easy global online commerce. However, cybercrime has grown right alongside it. Organized fraud has grown at a huge cost to digital businesses, individual consumers and society at large.

1. **Businesses facing fraud losses and rising operational costs:**
There is an increasing strain on internal fraud departments and mounting budgetary demands, without much to show for it. Fraud is still costing businesses billions each year in lost revenue and increased operational costs. When consumers fall victim to fraud on a digital business' website or app, it can damage a company's reputation and push the consumer to go to a competitor. For some businesses, especially those built upon peer-to-peer commerce and reviews, fraud can have a long-term impact on their profitability if customers lose trust in the integrity of their platforms.

2. **Impact on Consumers:**
Due to widespread acceptance of stable fraud levels among businesses, there are many individuals who are impacted by fraud. Consumers, who have their accounts hacked into or payment credentials misused, are left with the headache of trying to reclaim losses and take steps to secure their digital presence once again. This can lead to financial and emotional hardships for individuals.

3. **Wider Society:**
Fraud is often connected to malicious activity with far-reaching socio-economic impacts. For example, the abuse of digital channels and shared economy marketplaces to launder illegal money or fund terrorist and other criminal activity. As well as using fraud for new monetization avenues, social platforms have been abused for political gain from nation states looking to sway public opinion and tamper with elections.

Beyond Digital Identity

Digital identities have been corrupted at scale, in the wake of data breach after data breach; and by gaining insight into behavioral patterns from unauthorized access into user accounts during previous attacks. Therefore, fraud detection parameters that are trained to detect trusted or malicious behavior from a particular digital identity can be fooled by fraudsters. Data-driven fraud prevention needs an extra, robust layer that roots out fraudsters while allowing true customers to prove they are legitimate.

TRADITIONAL SOLUTIONS ARE NOT WORKING

The industry has been struggling with a lack of truly effective authentication solutions. Many options either have too much impact on user experience or can be circumnavigated by fraudsters en masse. For example, solutions such as CAPTCHA not only alienate customers as they have a success rate as low as 65% among genuine users, but fraudsters can also deploy low-cost image processing tools which categorize third-party visual data and trick the system into accepting bogus responses en masse.

As a result, there is heavy reliance on friction-free, risk-based authentication. This is an integral component of any fraud prevention strategy. However, fraudsters increasingly have the knowledge, tools and data to evade detection from data-driven security parameters.

Current fraud detection techniques rely on data that attackers can manipulate. They are able to use inexpensive tools and abundant identity information to emulate good customers, which increases false negatives and makes them exponentially harder to detect without inadvertently blocking legitimate users.

LEGACY CAPTCHAS

Many businesses still rely on outdated, grid-based CAPTCHA systems to stop automated attacks. However, these have been entirely overrun by bots. Simple web searches reveal dozens of marketplaces that sell bots guaranteed to bypass these defenses, some for as little as $20/year! Many even come with customer support functions to help fraudsters deploy them in the optimal way. Furthermore, many CAPTCHAs function as "black boxes" feeding no actionable insight or data back to the client about why certain attacks got through and how to mediate them. Couple that with the poor user experience that legacy CAPTCHAs provide, and it's clear they are largely ineffective in the modern, digital world.

THE GROWING GRAY AREA

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 can be faked.

There is an increasingly 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 the whole fraud prevention model off-gear. Fraudsters understand how these systems work and use this knowledge directly against the businesses they attack.The balance of power is with the fraudsters.

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

> The Arkose Labs solution has made a marked difference in protecting our online gaming platform against abuse. Arkose Labs has reduced fraud, without adding any friction for our users—an important criteria for the success of any online gaming platform.
>
> —Gaming Company

ARKOSE LABS: OUR CORE PRINCIPLES

To effectively manage fraud and abuse in this rapidly evolving ecosystem, businesses need a long-term approach that evolves with attack patterns, rather than a perpetual cat and mouse game. 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 good customers.

Arkose Labs has a vision for a world of zero-tolerance for fraud. This approach is based on the following core principles:

1. Undermine the economic incentive of fraud so it ceases to be a lucrative business. While there is still money to be made, fraudsters will find a way to do so by switching tactics, techniques and targets - until their profits are slashed by preventions which render attacks time-consuming, difficult and expensive.

2. Combine risk-based authentication with targeted friction. Intelligent step-up challenges are vital in order to stamp out automated and sweatshop-driven attacks at scale.

3. Stop fraud long-term, beyond deflecting individual attacks. To address fraud in the long-term, controls need to be adaptive, and continuously evolving. By constantly moving the goalposts on how to pass authentication challenges, it means that fraudsters cannot learn to circumnavigate them at scale.

4. Shift the attack surface away from the businesses fraudsters target. Independent verification of identity avoids draining in-house fraud prevention resources and provides a buffer between the fraudsters and the sites they are so practiced in attacking.

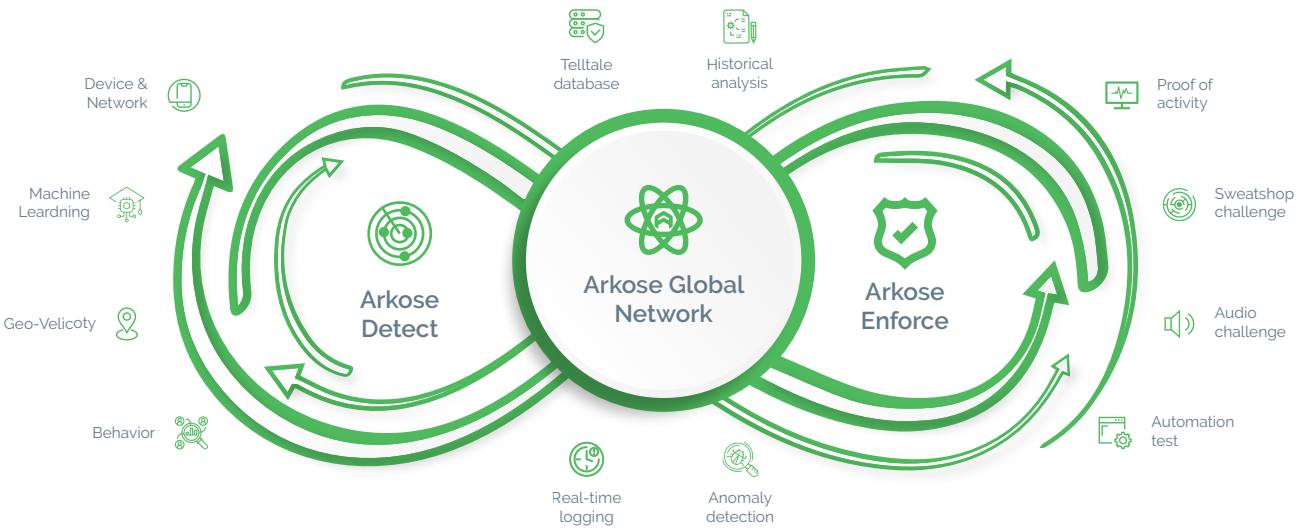
FRAUD AND ABUSE PREVENTION PLATFORM

The Arkose Labs Fraud and Abuse Prevention Platform combines real-time intelligence, rich analytics and adaptive step-up challenges to progressively diminish the profitability of attacks while adapting to evolving attack patterns.

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

Suspicious traffic is presented with incrementally complex challenges that demand time and extra resources to clear the challenges at scale. This permanently disrupts the economic viability of organized attacks and breaks the fraud model to stop both human and bot-driven attacks.

ARKOSE LABS FRAUD AND ABUSE PREVENTION PLATFORM



ARKOSE DETECT

Arkose Detect is a dynamic risk engine that analyzes data from user sessions & their interaction with technology. It unearths behavioral patterns across devices & networks in real-time. Combining this real-time digital intelligence with behavioral patterns, it 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 device validation to understand the characteristics and assess the validity of the device.

- **Continuous intelligence:** Combine digital intelligence with behavioral patterns that help unearth the underlying intent of a user and segregate users into smaller groups with distinct underlying motivations.

- **Location assessment:** Identify when fraudsters try to spoof their location. Increase suspicion of levels of activity disproportionate to authentic traffic from the location.

- **Abnormality detection:** Analyze the network traffic patterns in real-time to identify behavior patterns across cohorts.

> Arkose Labs not only helped reduce the ATO attempts but also provided us with a future proof way to protect against evolving attacks
>
> —FinTech Platform

- **Behavior biometrics:** Analyze user interaction with their devices to identify anomalies & automation.

- **Automated 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 businesses to help Arkose Detect correlate attack patterns across use cases and industries to understand how attacks are orchestrated. This network intelligence provides valuable insights in detecting anomalous behavior & 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:** Deep tell-tales to identify persistent sophisticated attackers through their interaction patterns.

- **Dashboard and visualization:** An intuitive dashboard to deliver insights as well as visualization and data stitching to deliver end-to-end insight across the customer journey. This unifies user data with real-time user behavior and metadata.

ARKOSE ENFORCE

Arkose Enforce delivers adaptive step-up challenges that accurately distinguish among 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. The challenges are designed with the latest innovations in machine vision technology in mind, meaning they cannot be solved by bots. Meanwhile, human sweatshop workers face increasingly complex challenges, which increases their time spent solving them and wastes the fraudster's resources when trying to clear challenges at scale. Since increasing costs diminish the profitability of the attack, fraudsters are compelled to stop.

Some of the challenge types include:

Basic bot challenge: Identifies basic automated attacks and blocks that traffic.

Acid test: Triages between a trained bot and a human with a test that uses new, untrained images and puzzle types in a challenge. This causes the automated processes to instantly fail while malicious humans succeed.

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, for example 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.

Key features of Arkose Enforce include:

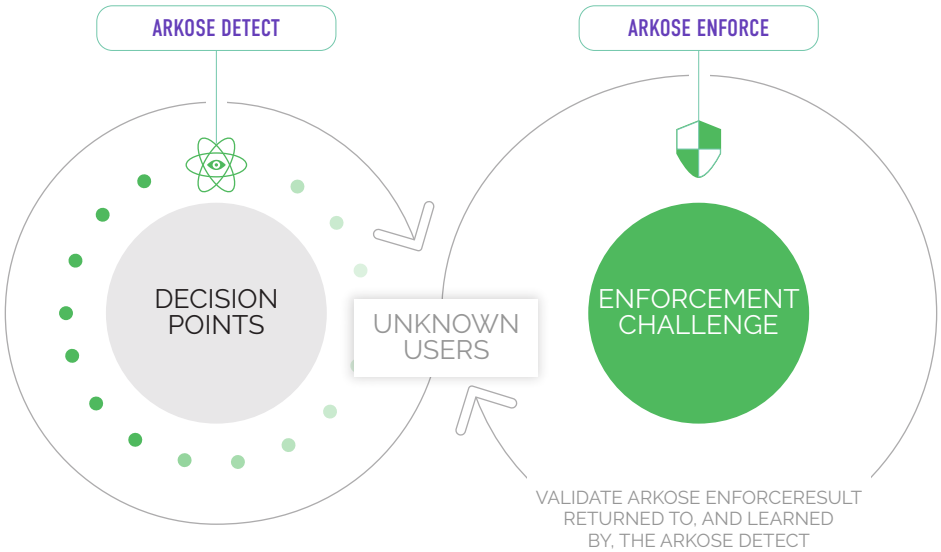
- **Bespoke and brand-integrated:** Arkose Enforce challenges are created using brand elements that blend with the overall branding of the website or app. This prevents disruption to the user interface and helps deliver seamless user experience.

- **Self-optimized step-up:** Using real-time insights from Arkose Detect and combining it with the risk profile of the user, the dynamic defense protocols automatically step-up 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 breaks the economics of the attack and 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.

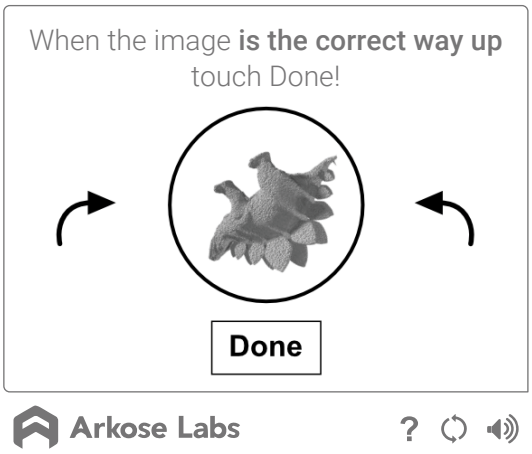
- **Accessible:** Arkose Enforce challenges are Section-508-compliant which helps ensure people of varied abilities across 31 languages can respond.

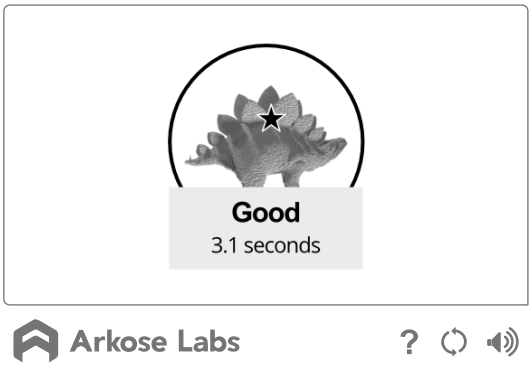


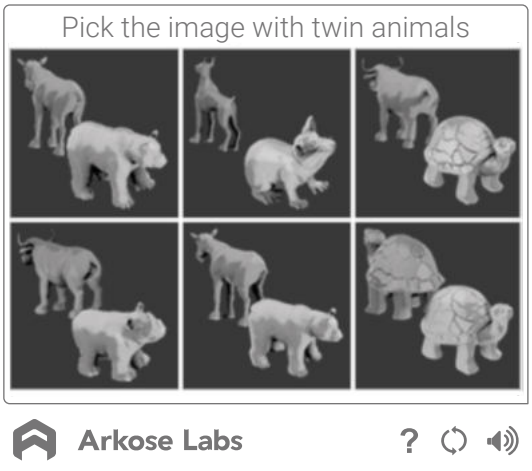
Arkose Detect and Arkose Enforce work seamlessly together and inform one another for improved future prediction and identification of malicious traffic. Deploying machine learning further sharpens anomaly detection and trains the platform in real-time, with the challenge as the feedback loop.

STOPPING BOT ATTACKS IN THEIR TRACKS

In some challenges, the user is asked to turn an image the correct way up. The nature of the images makes it easy for a human user to determine which is the correct way up, for example an animal that appears to be standing upright on its feet. The user only needs to complete one puzzle in order to solve the challenge. The image is generated in a way that takes advantage of weaknesses in machine vision attack tools, meaning fraudsters cannot use standard machine vision algorithms to fool the challenge response mechanism. This drastically increases the associated cost and expertise needed by the attacker as they will need to develop a toolset and modeling algorithm specifically targeting the Arkose Labs Enforce. Effectively, this stops bot attacks, because the appeal of using bots is they are cheap and easy to deploy. Spending time writing a custom-algorithm to defeat one specific challenge is not worth a fraudster's time or money.







Arkose Labs Acid Test

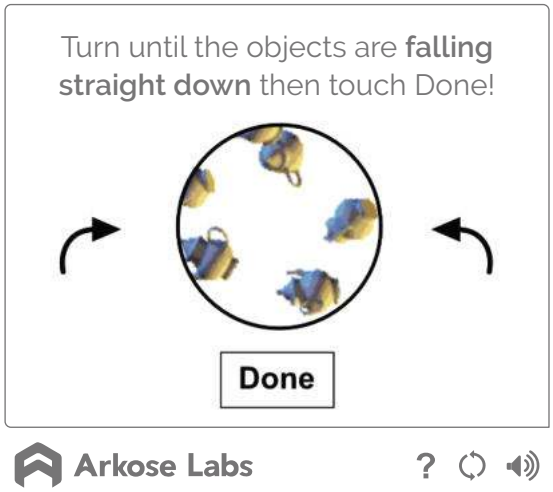
Many sophisticated bots can accurately mimic human traffic and go undetected by traditional solutions. While Arkose Labs' step-up enforcement can detect and stop most large scale bots, sometimes the fraudsters deploy bots that have been trained to act like humans. These bots behave like humans but have solve patterns that are closer to automated traffic. Upon detecting the presence of such bots, Arkose Labs deploys a proprietary 'acid test' to effectively triage the traffic into humans vs. bots. This starts with the platform switching out the one visual puzzle for a completely new kind of puzzle, still easy for humans to solve. This effectively stops all automated traffic, as the attack program cannot possibly solve a puzzle its designer has never seen before.

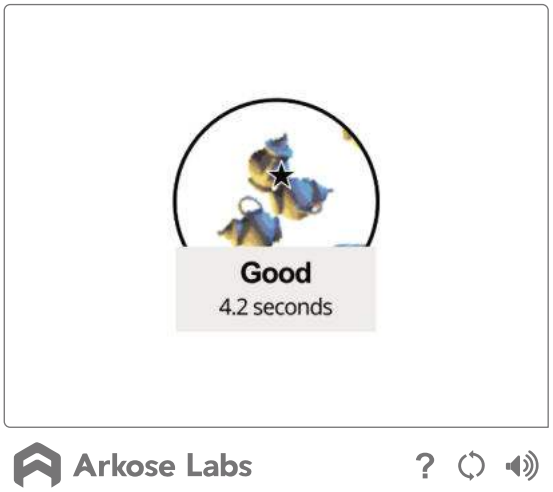
Once the bots have been identified, the challenge is switched to a new type that would not be solved by the bots without additional training.

> We analyzed the problem internally and deployed fraud prevention solutions without much success. We then approached Arkose Labs and within a few days fraud rates dipped dramatically. Arkose Labs has helped us maintain customer relationships, so crucial in growing a business like ours.
>
> —FinTech Platform

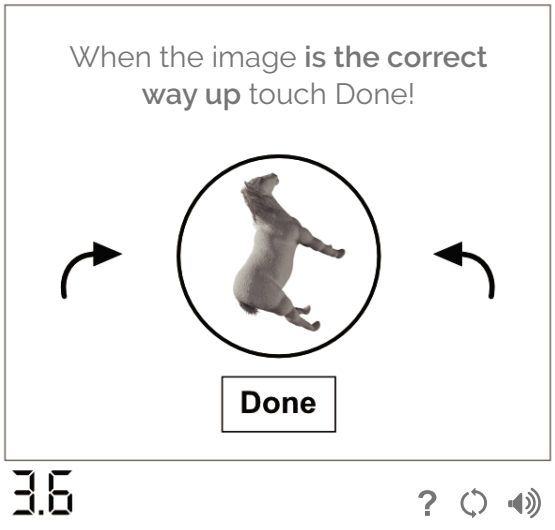
PUTTING HUMAN FRAUDSTERS IN QUICKSAND

In the event a higher suspicion level is detected, the user is asked to take a completely different kind of puzzle, for example, to turn an image until the objects in the animation are falling straight down. If the user is good, he or she only needs to complete one puzzle in order to solve the challenge.



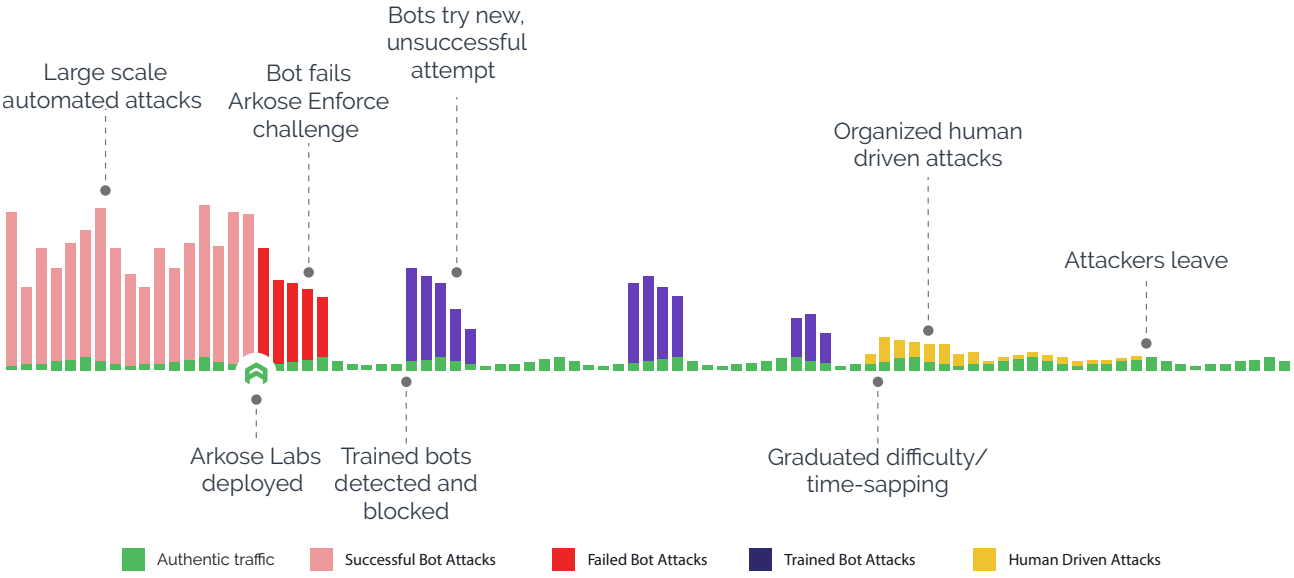


However, when the platform detects signals that a sweatshop -- that is, a large amount of humans who are employed to conduct a coordinated attack on behalf of one fraudster -- is behind an attack, they are presented with a series of challenges that are designed to make these clickfarm operations expensive and unsustainable by wasting their time. Depending on data intelligence and solve patterns of the click farms, these challenges can either be timed (to stop queued solve pipelines) or take a long period of human attention to solve (to sap user efficiency).



Arkose Enforce also dynamically chooses the number of challenges presented for any given session based on the risk decisioning (within the limits specified by the customer). This is especially useful in sapping the efficiency of human sweatshops and click farms.

ATTACK EVOLUTION



100% SLA GUARANTEE

The solution is powerful and accurate enough to make Arkose Labs the first and only cybersecurity company to guarantee efficacy with a Service Level Agreement (SLA) on its primary function: preventing all automated fraud and abuse on its customers' websites and apps.

For too long, businesses have been accepting fraud as a 'cost of doing business'. The only long-term way to stop cybercrime is to adopt a zero-tolerance approach which focuses on disrupting the underlying economic drivers of fraud.

Companies on the Arkose Labs Fraud and Abuse Prevention Platform benefit from this zero-tolerance attitude, with a 100% SLA guaranteeing the efficacy of the platform in remediating large-scale fraud attacks.

Arkose Detect & Arkose Enforce work seamlessly together to differentiate between good and malicious traffic with unprecedented accuracy. Requests that cannot be verified by Arkose Detect are challenged with Arkose Enforce and not blocked. Secondary screening ensures that unrecognized requests of human origin are always afforded the right to prove their authenticity. As a result, it never blocks legitimate humans and there is no negative effect on user experience or throughput rates.

COMMERCIAL ASSURANCE AGAINST CREDENTIAL STUFFING

Arkose Labs is the first vendor to back its customers with a $1 million limited warranty that covers response expenses in the event of a successful credential stuffing attack.

ARKOSE GLOBAL NETWORK

Arkose Detect and Arkose Enforce are supplemented and made more robust by data and network intelligence from the Arkose Global Network. This is data gleaned from our global base of dozens of clients in many different industries. So, for example, the telltales of a fraud attack seen against one client will be noted and if spotted against another client will be easily detected and stopped. In this way the Arkose Labs platform is able to constantly learn and combat evolving threat patterns.

Using this network intelligence, the platform is able to draw upon previous attacks from its proprietary telltale database to detect and stop them when they appear again, and identify and root out anomalous behavior as it appears in digital traffic. All Arkose Labs clients benefit from this sharing of data.

Key Features of Arkose Global Network include:

- **Proprietary telltale database:** Repository of known fraud and abuse telltale signals, which are made up of a clustering of information from 300+ data points from a single user session.
- **Historical attack pattern calibration:** 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 emerging attack patterns.
- **Real Time Logging:** Detailed logs of user activity provided by Arkose Labs servers. Each user session is tagged with a unique token, which includes telemetry data about the user, such as what we have learned from the user's presence elsewhere on the Arkose Labs Network, and the suspicion level for each user.
- **Managed Services:** Our team of customer support analysts is always on hand to provide actionable insight from the data to our clients.
- **Data Exchange:** Data passed between the Arkose Labs servers and the customer's servers, based on predefined parameters, in order to better determine risk assessment or friction level.
- **Truth Data API:** Seamless feedback loop with customer truth data that enables the Arkose Labs system to be continually refined.

> We had very specific requirements as to how we wanted Arkose Labs to approach stopping the attacks. They are very flexible in tailoring attack mitigation techniques that align with our own unique security strategy.
>
> —Gaming Platform

KEY COMPETITIVE ADVANTAGES

- **Shifting the attack surface:** Arkose Labs' approach shifts the attack surface from the business to Arkose Labs' independent platform. As a result, fraudsters are no longer attacking their targeted customer touch points but are diverted to a third-party platform in order to sap their resources. Businesses do not need to then expend their own resources to deal with attacks and they benefit from shared attack intelligence from across the Arkose Labs customer network.

- **Deep analytics to detect sophisticated fraudsters:** Recognizing that fraudsters have insights into existing fraud detection solutions and the tools to circumvent those defenses, Arkose Labs takes an approach that can identify patterns and tell-tales as fraudsters try to launch these attacks. By moving from looking at the static identifiers and focusing on the fraudsters' behavior and interaction with the technology, Arkose Labs can identify even the most sophisticated attacks. Arkose Detect is augmented with Arkose Labs' automated traffic auditing tools that constantly assess its accuracy, allowing it to be constantly refined.

- **Breaking down the fraudsters' business economics:** Arkose Labs' approach makes attacks more difficult and costly, which disrupts the fraudsters' economic incentive and breaks their business model. This results in a long-term solution and stops the cat and mouse game that fraudsters play with businesses.

- **Data network effect:** The Arkose Labs network analyzes 10 billion transactions, across 2 billion devices and 5 billion IP addresses, and has more than 20 million hours of enforcement challenge interaction intelligence. Each company on the network benefits from this visibility, as each attack provides insights into the fraudsters' operations and augments the overall network intelligence.

- **Collaboration and Information sharing:** Since fraudsters want to make money as fast as possible, they quickly pivot each time their attacks are thwarted. With Arkose Labs, they are unable to bypass the platform and end up wasting resources in their attempts. While most fraudsters simply move on to try to attack other businesses, collaboration across a broad range of companies ensures that tell-tale signs of specific attacks are shared within trusted circles. This results in a win for the entire digital commerce ecosystem as there is one less operator trying to dupe businesses and customers.

- **Continuous learning:** The platform continually learns from newer attack patterns. This shifts the power from the fraudsters to the businesses, and benefits the overall digital commerce ecosystem.

HOW DOES ARKOSE LABS KEEP YOU ONE STEP AHEAD OF CYBERCRIMINALS?

1. The Acid Test

The Arkose Labs Acid Test is an automated experiment conducted by Arkose Enforce. The programmatic test introduces uncharacteristic visual data into the challenge–response mechanism, which causes automated processes to spontaneously fail. The Acid Test spots inauthentic traffic and extracts critical threat intelligence that enables Arkose Labs to remediate abuse within a guaranteed period.

2. New Puzzle Types

Fraudsters have learnt to circumnavigate other image-based authentication steps at scale. They use low-cost image processing tools to categorize third-party visual data, providing responses that can fool visual challenge-response technologies. In contrast, responses to Arkose Enforce are generated from proprietary visual data that has no residual benefit to computer vision for training machine learning models. These secure responses augment in real-time and prevent attackers from anticipating how Arkose Enforce will behave in future. Arkose Enforce prevents automation at-scale and increases the operational costs for attackers. Puzzles are adaptive and change incrementally. Effective solutions are those which keep moving the type of challenge presented in order to keep moving the goalposts and prevent fraudsters scripting their way round your preventions.

3. Bug Bounty Program

An exclusive private bug bounty program with Bugcrowd, the #1 crowdsourced security platform, provides continuous assurance of the stability and strength of the various product features that make up the Arkose Labs system. This program provides access to elite bounty hunters, with a skilled testing pool tailored towards eliminating account takeover attacks, fake user registrations, and other types of fraud and application abuse.

Utilizing crowdsourced testing as an additional validation step during development enables Arkose Labs to test features against 'real world' attackers and gain insight into how attackers approach an attack on the company's system.

DEMONSTRATED RESULTS

The Arkose Labs approach has proven efficacy, with more than $100 million in fraud saved for customers over the last twelve months. The platform thwarted over 500 million fraud attacks this year, ranging from account takeover, fake account registration and payment attacks across diverse industries. Industry recognition includes awards from SC Media, MRC, SINET, RSA Conference and Cyber Defense Magazine, as well as being named a 2020 “Cool vendor” by respected industry research and analyst firm, Gartner.

CASE STUDY: MICROSOFT OUTLOOK.COM

Microsoft Outlook needed a new way to stop fraudulent new account creations while improving customer experience - all in a cost effective manner. This was important not only to protect their own users but to create a safer environment for the wider ecosystem.

Microsoft deployed the Arkose Labs platform to differentiate between good users, bots and malicious humans in order to eliminate spam and abuse. New users were shown enforcement challenges when sending their first email. The team implemented custom rules and policies to detect anomalous and suspicious behaviour, with challenges being presented whenever there was evidence of downstream large-scale abuse or spam. The result was a 33% improvement in good customer throughput. There was a 93% reduction in fraud and abuse, with malicious users being prevented from carrying out large-scale attacks after setting up new accounts.

IMPLEMENTATION

JavaScript-based implementation with the client and server-side components makes it easy to implement the solution. The majority of new Arkose Labs customers onboard within three weeks.

CONCLUSION

Fraud prevention has traditionally honed in on assessing users by their digital identity, based on the devices they use, the locations they transact from and their associated identity credentials. However, in a world where data breaches are commonplace and digital identities have been corrupted at scale, a new approach to combat fraud is needed. That’s because there is enough data and technology at fraudsters’ disposal to masquerade as individuals and spoof their devices and locations with devastating accuracy - using knowledge of current fraud controls directly against businesses they attack.

While many businesses have come to accept fraud as an operational cost of doing business in the digital age, Arkose Labs believes that the only long-term way to stop cybercrime is to adopt a zero-tolerance approach which focuses on disrupting the economic drivers of fraud.

The Arkose Labs Fraud and Abuse Platform does not just mitigate the effects of fraud but provides powerful remediation which blocks 100% of automated traffic, and enables businesses to deflect attacks from skilled cybercriminals and sweatshop outfits.

Its innovative approach combines a powerful decision engine (Arkose Detect) with enforcement challenges (Arkose Enforce) that incorporates interactive gamification and machine vision, and supplemented by vast network intelligence (Arkose Network). This allows good users to maintain the seamless digital authentication experience they have grown accustomed to, while providing friction and frustration to fraudsters.

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.

Mail:

support@arkoselabs.com

Address:

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

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

United Kingdom • 167-169 Great Portland Street, 5th Floor, London, W1W 5PF

Schedule Demo