Arkose Labs

The Advantages of a Truly Secure Arkose Enforce Capability in Fraud and Abuse Prevention

An Arkose Labs White Paper

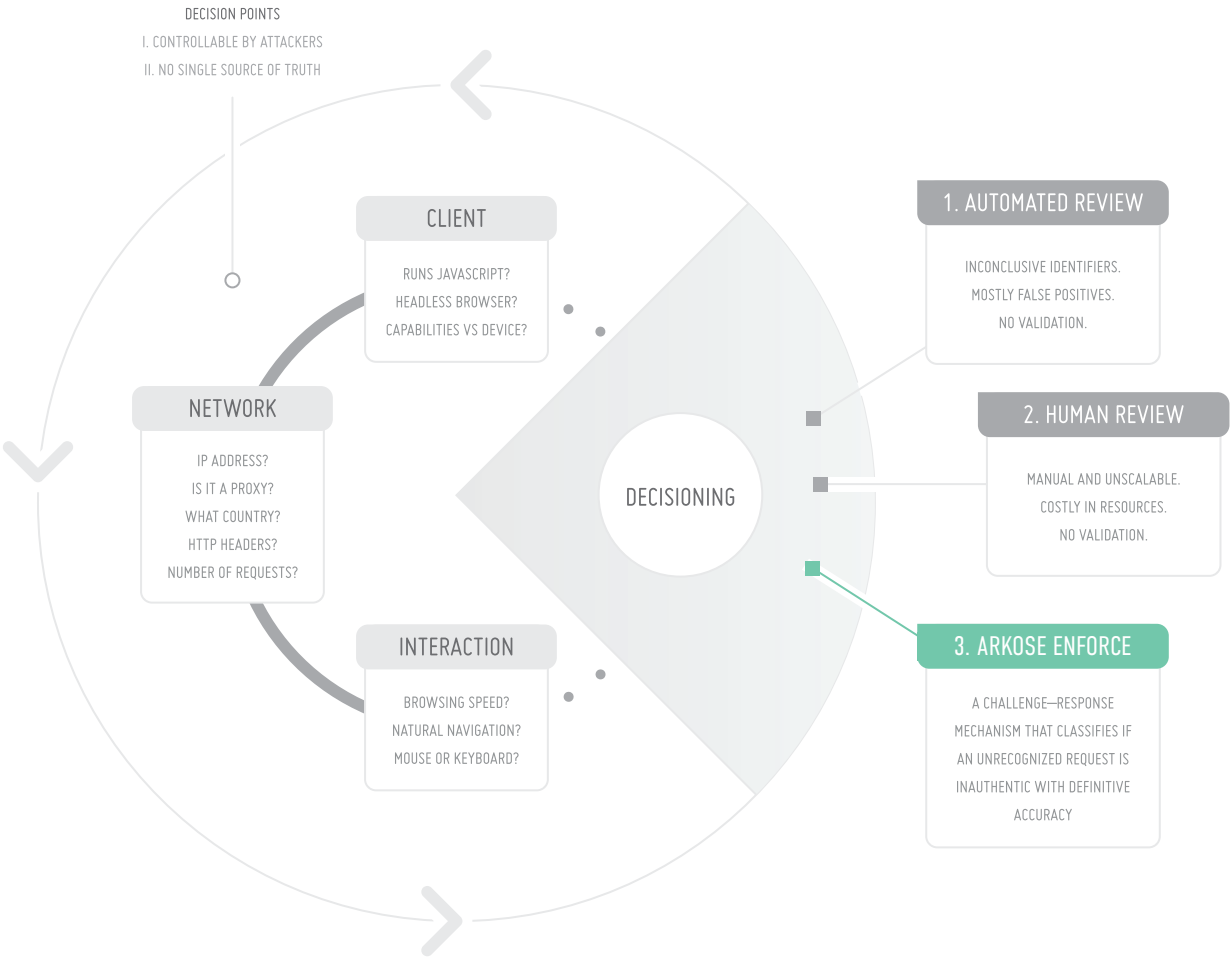
Contents

Introduction

Today's best-effort tools for online fraud detection are all built with the same fundamental architecture. These systems gather multiple data points on endpoints, and monitor behavior to come up with what amounts to a risk score for each user. These risk scores rarely present a clear good vs. bad determination, but rather a continuum of probability. This leaves Enterprise customers in the difficult position of needing to make a decision based on a probability score, which does not give them the confidence they need to block potentially-malicious users without the added risk of blocking legitimate customers.

These tools do help stop unsophisticated attacks, like so many other security products, although with advanced fraud — like account takeovers — there is a strong financial motivation, and attackers will continue to find ways around simple risk profiling methods.

FIGURE 1.0 APPROACHES TO FRAUD AND ABUSE DECISIONING



Fraud and abuse mitigation systems were previously built with the baseline assumption that there is no way to truly tell a machine from a human. That assumption leads to multiple design trade-offs that fundamentally limit the efficacy of those products. Revisiting this assumption leads to an immediate breakthrough in fraud prevention efficacy, and sets the stage for machine learning systems that will fundamentally change how we think about fraud and abuse prevention.

Current Approaches

There are several limitations to the standard behavioral analysis and risk scoring approaches. False positive determinations block users and lose revenue. These blocked users either have no recourse, or must use expensive customer service channels to appeal their reputation. On the other hand, false negative determinations facilitate access for bad actors and result in fraud. Consequently, some vendors advocate using a system in which the Enterprise biases the good vs. bad decision by assessing the sensitivity of data being accessed. This questionable approach does not provide a conclusive solution to the problem, but rather tries to mitigate the associayed damage. Without an effective Arkose Enforce mechanism, the good vs. bad decision is either an educated guess, or subject to expensive and inconclusive manual human review.

Moreover, a risk score with no validation from an Arkose Enforce challenge has an exponential decline in value over time as attackers continually find—and share—new ways to subvert the risk assessment. When the attacker is given a clear feedback signal as to whether or not they have successfully evaded Arkose enforce, the attacker may iterate and tweak the attack until it passes. Enterprises have previously tried to address this challenge using technologies like Google reCAPTCHA to provide an Arkose Eforce capability, but those are easily bypassed using off-the-shelf software.

An additional problem with using a third-party Arkose Enforce is the lack of interaction between the risk assessment component and the challenge itself. This results in two unconnected systems sharing responsibility for Arkose Enforce. In the absence of a dynamic feedback loop between the risk assessment and challenge, a motivated attacker need only subvert one component to bypass the system.
Finally, Arkose Enforce introduces a friction point for customers that compounds the problem by turning away legitimate users, while doing little to stop attacks. A new approach is needed.

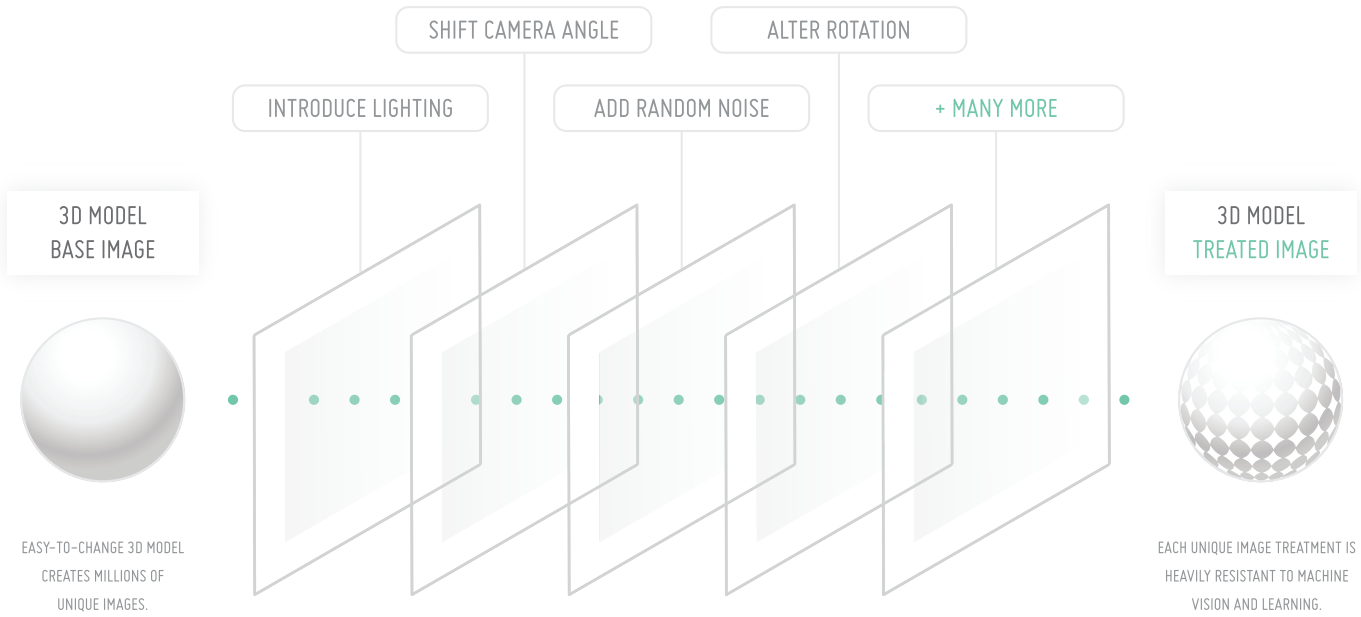
A New Approach

There is now a third option beyond the traditional allow vs. block approach. By having a truly secure and reliable Arkose Enforce capability, suspicious traffic can be challenged with certainty around the result. This new Arkose Enforce capability is simple for the human brain—presenting no friction to legitimate users—and remains incredibly difficult to subvert thourgh automation. A truly secure challenge radically changes the economics of automated fraud and abuse.

The new approach includes millions of security images orchestrated from three-dimensional models, with each challenge containing a visual subject that is uniquely generated for that user. The design of the Arkose Enforce challenge intentionally avoids problems that are solved by commercial off-the-shelf software This forces attackers to engage expensive counsel on machine vision and machine learning in order to bypass the challenge at scale. When attackers try to use common machine vision software to analyze the images, the results are consistently incorrect. For example, an image perceived to be an animal by a human is classified as a cloud, or fog, by software.

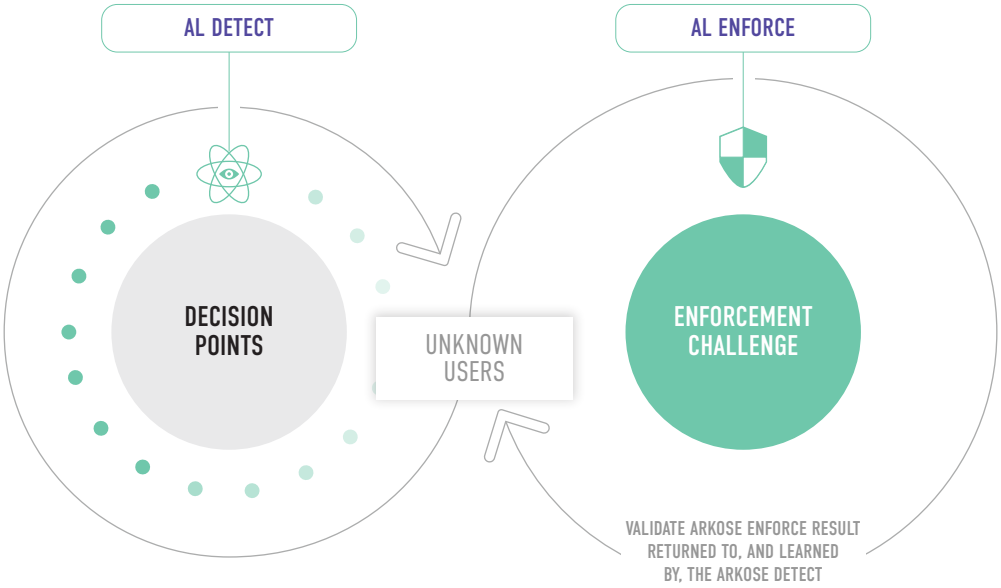
While it may be technically possible to solve this type of Arkose Enforce challenge with sufficient resources, this new approach also facilitates quick changes to the challenge that easily render the work done by the attackers useless. With the ability to change the Arkose Enforce challenge regularly and rapidly, the attackers never see a return on their now-significant investment in attempting to automate challenge completion.

FIGURE 2.0 EXAMPLE OF VISUAL ORCHESTRATION IN ARKOSE ENFORCE CHALLENGES



An important benefit of this truly secure challenge is that it radically improves the efficacy and decisiveness of a risk assessment feedback routine. Now that the challenge discerns with certainty whether a user was human or not, there is an opportunity to automatically train the Arkose Detect with an immense volume of immediate and accurate feedback. Improving the Arkose Detect in this way results in superior decisioning, and facilitates the ability to show challenges only to suspicious users. This reliable decisioning only works when the challenge is truly secure.

FIGURE 3.0 SELF-TRAINING ARKOSE DETECT FEEDBACK LOOP



Implications of this New Technology

This new technology can be used in an Enterprise environment in a number of important use cases, including: Account Takeovers, Spam, Blocking Transactions, Ticket Scalping, Game Hacking, Fake Users, Carding, Auction House Abuse, Fake Ratings and Scraping. The following example illustrates how this technology solved a problem with Single Request Attacks for a major airline.

Single Request Attacks are behind the most advanced automated abuse seen today. Each request is commonly made by a headless browser, executes JavaScript like a legitimate human user, presents a dynamic client fingerprint so the device cannot be identified, and offers a dynamic network fingerprint so the IP address cannot be identified. The impact of such attacks was significant to the airline, and traditional products were unable to mitigate—or prevent—the problem.

Single Request Attacks use this systematic approach to decouple tell tales and obscure critical security breaches that bypass all other bot mitigation services, which rely only on threat scoring and passive monitoring. After implementing this technology, which uses a bilateral approach to combines a global Arkose Detect and a reliable Arkose Enforce challenge, the airline was able to eliminate a multimillion dollar fraud problem that precluded legitimate customers from purchasing tickets.

Another real deployment example is a leading messaging app that was crippled by immense spam. As user complaints stacked up, traditional approaches combined with unreliable Arkose Enforce technology were unable to solve the problem. The abuse was serious enough that it was leading to an increase in customer churn. Within weeks of implementing this new and truly secure technology, the associated complaint frequency dropped from 300+ million per month to zero.

Further Implications with Machine Learning

Incorporating a real-time validation capability to test machine learning algorithms provides an enormous advantage for the reliability of these systems. Machine learning systems in cyber security are commonly disadvantaged by limitations, such as small data sets of attacker behavior. By having a truly secure and reliable challenge mechanism, these systems can get real-time feedback at a pace and scale unavailable anywhere else. We are confident that research and investment in this area will lead to additional breakthrough technology advances that will solve important problems in fraud and abuse, as well as in a broad range of alternative use cases.

Conclusion

New technology that combines a global Arkose Detct with a reliable Arkose E nforce challenge can eliminate sophisticated fraud and abuse almost immediately—without adding friction to real users. This approach provides an immediate and significant saving to Enterprises across industries including retail, airline, gaming, ticketing, online marketplaces, travel and social. The technology is straightforward to integrate with existing systems, and allows Enterprises to verify the technology through a rigorous trial with minimal effort and expense. Enduring and demonstrable success with this technology has supported our offer of the industry's first 100% Service Level Agreement, guaranteeing automated attack remediation. Arkose Labs uses this new technology to solve multimillion dollar fraud problems for the world's most targeted businesses with zero friction to users.

Visit arkoselabs.com for more information about this technology and the 100% SLA.