Arkose Labs | SOLUTION BRIEF

Stop Account Takeover While Lowering Friction for Trusted Users

Overview

Digital economy is rapidly evolving with innovative technologies and disruptive business models emerging each day. As businesses offer innovative services, customers are increasingly relying on digital channels to open new accounts, shop, transfer funds, or seek loans. In the process, however, customers leave behind digital footprints—in the form of personally identifiable information—that are harvested by fraudsters through data breaches, phishing, malware, and so forth. Hiding behind the anonymity of the internet, fraudsters use all of this data for numerous frauds including account takeover.

ATO Obliterates Customer Relationships

Account takeover is one of the biggest challenges digital businesses face today. It not only causes financial and reputational losses to businesses but also obliterates the efforts businesses are making to meet rising customer expectations of friction-less access, personalized services, and instant payments.

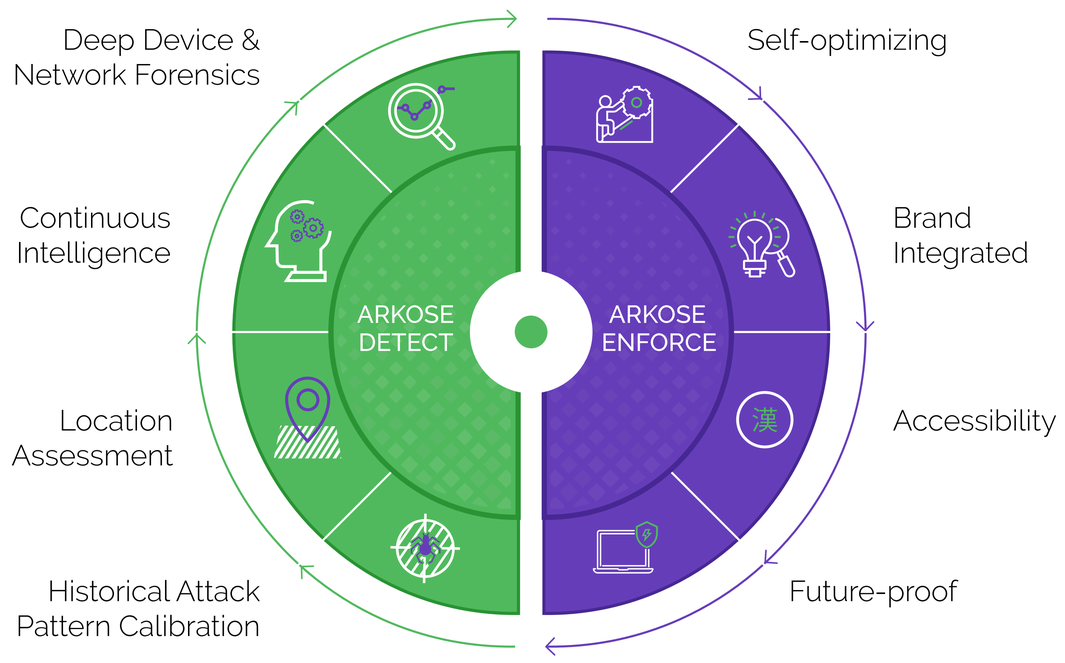
Digital businesses are trying every measure to build deep customer relationships and ensure customer delight—from promotional offers, to loyalty programs, rewards and so forth. However, tech-savvy fraudsters use the stolen customer credentials to take over accounts and drain money, reward points and other assets contained therein, access the saved payment details and/or passwords, and even use the compromised accounts as a launchpad for various other crimes. In the process the delicate business-customer relationship gets jeopardized.

Account takeover can be difficult to detect as fraudsters impersonate genuine customers and manipulate verification processes to avoid detection. Businesses run the risk of disrupting customer experience should they choose to introduce additional verification processes. Therefore, businesses need non-invasive solutions that effectively prevent account takeover attempts without impacting customer experience.

Fight ATO with Arkose Labs

The first step towards preventing account takeover is accurate identification of customer intent and segregation of malicious users from genuine users.

Arkose Labs solves online fraud and abuse problems for global brands with its Fraud and Abuse Prevention Platform, while delivering a seamless customer experience. The platform features a dynamic risk engine that accurately differentiates genuine customers from fraudsters by enforcing challenges to authenticate identity. Depending on the risk assessment of a user, the adaptive stepped-up Arkose Enforce challenges are presented. While genuine users can easily clear the challenges and access their accounts, this graduated approach breaks the economics of the attack for the fraudsters, making it non-viable.



Arkose Detect is Trained by Arkose Enforce Results

Arkose Detect

The multi-level integrated approach involves global Arkose Detect that analyzes data from user sessions to recognize users across networks, assign a risk profile, and intelligently serve an Arkose Enforce challenge such that only fraudsters are presented with multiple challenges.

The key features of the Arkose Detect are:

Deep Device Forensics

Digital intelligence that helps identify rogue devices and assess the risk and reputational integrity of a user to filter out fraudsters from a group of genuine users.

Intelligent Analytics

Analyze behavioral patterns and other digital intelligence to understand the underlying intent of a user.

Location Analysis

Process the information to determine the origin of the attack.

Pattern Correlation

Unearth patterns and correlate them with attack patterns from across use cases to demonstrate how attacks are orchestrated.

Arkose Enforce Challenges

Despite a complex mix of online traffic—originating from diverse device types and geographical locations—Arkose Labs solution can accurately identify bots and malicious human traffic from click-farms or sweatshops. The risk score assigned to a user helps present adaptive Arkose Enforce challenges. Greater the risk, more the stepped-up challenges presented. This forces the fraudsters to invest more time and additional resources to clear the challenges at scale, which in turn diminishes the returns from the attack and makes it less profitable.

The key features of the Arkose Enforce challenges include:

Self-optimized

Depending on the risk profile, the prevention models automatically step-up the challenges to stop the attacks.

Bespoke

The Arkose Enforce challenges are custom-made and blend with the brand elements to provide a seamless user interface.

Accessible

Section-508-compliant so that people of varied abilities can access the challenges in over 31 languages.

Adaptive

Regular updates and releases ensure that the challenges evolve with the changing attack techniques.

Conclusion

The Arkose Labs solution helps protect the sanctity of online gaming platforms and ensure meaningful gaming engagement for genuine players while breaking the attack economics for the fraudsters.

demo@arkoselabs.com
(800) 604-3319
arkoselabs.com

Schedule Demo