Arkose Labs | SOLUTION BRIEF

New Account Fraud

Arkose Labs provides long-term, effective protection against fake account creations.

Global businesses are seeing a prolific rise in fraudulent new account registrations. Account originations are the most attacked customer touchpoint on the Arkose Labs network, with a rise of 70% in bot-driven attacks over one quarter at the end of 2019. Traditional solutions not only alienate customers with a success rate as low as 65% among genuine users, but also fraudsters can easily trick the system into accepting bogus responses en masse.

Businesses need an intelligent approach that combines efficient user experience with robust defense against new account fraud.

Arkose Labs Solution for New Account Fraud

Arkose Labs' Fraud and Abuse Prevention Platform combines continuous risk assessment with tailored enforcement challenges to provide long-term, robust protection against new account fraud.

The Arkose Labs Fraud and Abuse Prevention Platform uses a two-step system: Arkose Detect and Arkose Enforce.

Arkose Detect is a global risk engine that analyzes in-depth digital intelligence about the user to understand underlying intent and provide risk scores.

Based on these insights, Arkose Enforce then delivers tailored enforcement challenges to suspicious users. The challenge-response mechanism adapts to the risk profile of a session and is highly effective at eliminating automated attacks and preventing fraudsters from scaling up human-driven attacks.

Genuine users can easily prove their authenticity, while fraudsters are deterred from creating new accounts in bulk due to the increase in time and resources needed to clear challenges. This slashes their ROI and causes them to abandon the attack.

Technology Highlights

- **Unified platform** based on continuous learning between risk-based and step-up authentication results.
- **Acid Test which differentiates** between human traffic and automated attacks.
- **Detailed risk profiling** using deep device and network forensics combined with behavioral analytics.
- **Targeted enforcement challenges** which adapt to the risk profile of traffic and stay ahead of evolving threats.
- **Effective protection against attack types, including single request attacks,** scripted attacks, trained bots and sweatshop activity.
- **Incremental friction** which saps fraudsters' time and resources and compels them to abandon attacks.

The Arkose Labs solution guarantees defense against large-scale, automated attacks, meaning that fraudsters cannot get enough economic return from new account fraud. Businesses who use the Arkose Labs platform can rest assured that they have the most resilient protection in place against this type of fraud.

Arkose Labs provides powerful protection against fake account creations

Fraudulent credit applications

Credential testing

Money laundering

Identity theft

Abuse of free trials

Spam

© 2021 Arkose Labs. All rights reserved.

The Arkose Advantage

100% attack remediation SLA: Arkose Labs is the only company to guarantee a solution which blocks all automated attacks and prevents fraudsters from attacking at scale.

Digital intelligence and forensics: Arkose Labs provides sophisticated risk profiling using historical behavior analytics, sharing outcomes across the customer network.

Real-time protection: Graduated risk-based friction evolves with attack patterns and allows legitimate users to prove authenticity without negatively impacting user experience.

Self-optimizing platform: Constant feedback loop between Arkose Detect and Arkose Enforce constantly improves fraud detection rates with fewer challenges.

Future-proof protection: Long-term remediation renders fraud unsustainable and unprofitable, compelling fraudsters to abandon attacks.

Implementation

Arkose Labs is easily incorporated into existing infrastructure. It becomes an extension of your security and fraud teams without server-side proxies, daily intervention, or external systems.

The solution is user-friendly, with JavaScript-based applications for both client and server. Most new Arkose Labs customers fully integrate the solution within three weeks.

Results

Slash fraud losses: Detects and blocks human and bot-driven attacks to reduce fraud by 50-90%.

Streamline authentication: Secondary screening which appears in band for a seamless user experience.

Block sweatshop-driven attacks: Proactively identify traffic originating from organized sweatshops and click farms.

Conclusion

Arkose Labs provides long-term, intelligent protection against new account fraud. Arkose Labs is the only provider on the market offering comprehensive fraud prevention that seamlessly combines data analysis via Arkose Detect, with tailored step-up challenges created by Arkose Enforce.

These challenges significantly increase the time and resources needed to carry out account registration attacks, rendering them financially non-viable for fraudsters. Genuine users, on the other hand, enjoy a seamless sign-up experience and can transact safely and securely on websites and apps.

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

Schedule Demo

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.

© 2021 Arkose Labs. All rights reserved.