Arkose Labs | SOLUTION BRIEF

Payment Fraud

Future-proof protection against evolving payment fraud attacks

Payment fraud is a lucrative business for cybercriminals, causing billions of dollars' worth of annual losses to businesses around the globe. Many businesses tolerate fraud losses as a 'cost of doing business' in the digital age, fearing that more robust security measures will introduce friction and negatively impact conversion rates. Unfortunately, this perpetuates the problem by providing the financial incentive for fraudsters worldwide.

Organizations need a smarter approach that can help them strike an optimal balance between user experience and defend against large-scale fraud and abuse.

Arkose Labs Solution for Payment Fraud

The Arkose Labs Fraud and Abuse Defense Platform combines risk-based decisioning and intelligent step-up authentication to slash payment fraud rates. Real-time risk assessments inform a unique challenge-response system, which delivers targeted friction in order to eliminate unauthorized payment attempts.

The Fraud and Abuse Defense Platform uses a combination of Arkose Detect and Arkose Enforce. Arkose Detect carries out real-time risk assessment of users. Using deep device and network forensics in conjunction with behavioral patterns, Arkose Labs validates third party signals, which help prevent unauthorized payments and fund transfers, without disrupting the user experience for authentic users.

This digital intelligence informs Arkose Enforce, which then presents unique enforcement challenges to risky traffic. The challenge-response mechanism adapts to the risk profile of a transaction and is highly effective at eliminating automated attacks and preventing fraudsters from scaling up human-driven payment fraud.

Genuine users have an opportunity to prove their authenticity but fraudsters are forced to spend more time and resources clearing authentication challenges at scale. This slashes potential profit for fraudsters, compelling them to abandon the attack.

Technology Highlights

- **Sophisticated risk profiling** triages traffic using deep device and network forensics.
- **Dynamic risk score** informs the platform on when to present step-up challenges.
- **Enforcement challenges** are tailored towards the specific risk profile to root out bots, sweatshops and fraudsters.
- **The nature and complexity of challenges adapt** intelligently and keep ahead of evolving threats.
- **A self-optimizing platform,** which is based on continuous learning from risk-based and challenge-response intelligence across 15+ billion transactions.
- **Historical attack pattern calibration** helps unearth and correlate patterns across use cases and industries for more accurate anomaly detection.

Arkose Labs provides powerful protection against evolving payment fraud patterns.

CNP transactions using stolen card details

Gift card abuse

Unauthorized money transfers

Abuse of stored payment details accessed through account takeovers

The Arkose Advantage

100% attack remediation SLA. Arkose Labs is the only company to offer a guarantee on stopping all automated payment attacks.

Graduated risk-based friction, which evolves with the attack patterns and ensures legitimate users have an opportunity to prove their authenticity.

Self-optimizing platform which uses the feedback loop between risk decisioning & enforcement to continually fortify the platform against evolving threats.

Future-proof protection designed to render fraud unsustainable in the long-term.

Shifts the attack surface away from the business, with the Arkose Labs platform acting as an intermediary to authenticate a transaction.

Results

Fraud Elimination: Detects & blocks both human & bot-driven attacks to reduce fraud by 50-90%.

Higher Customer Throughput: Increases good customer throughput by 15-25%.

Real-time Remediation: Adaptive, step-up challenges that include machine & human-specific challenges to effectively disrupt the techniques fraudsters use without disrupting user experience for valued users.

Implementation

Arkose Labs integrates seamlessly into existing infrastructure. It becomes an extension of your security and fraud teams without reverse proxies, daily rule setting, or third-party infrastructure.

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

Conclusion

The Arkose Labs solution provides digital businesses with complete protection against payment fraud. Using a long-term remediation approach, Arkose Labs breaks the economics of the attacks by dramatically increasing the time and resources needed to carry out successful attacks. This renders attacks financially non-viable for fraudsters, while ensuring good customers can complete transactions in a simple and secure manner.

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.