

SHARING ECONOMY

Effectively securing peer-to-peer platforms

The sharing economy has upended traditional business and commerce, allowing people to rent housing, use vehicles, loan money and exchange any number of services directly with one another.

As sharing economy platforms have risen in popularity, they've been hit with a rise in fraud as well. Bad actors pose as fake consumers, hack into legitimate accounts and set up bogus profiles as a service provider in order to scam and cheat real users of these platforms. Trust is critical to the continuing success of the sharing economy, which is why securing these platforms from malicious actors is of the utmost importance.

Arkose Labs Solution for the Sharing Economy

It's critical for sharing economy platforms to root out fraud without placing too big a burden on good users. It's the usability and seamless experience of these services that makes them so appealing. That experience cannot be lost in the process of fighting fraud.

Arkose Labs' solution is one that's tough on bots and human fraudsters, but easy on good users. We take a zero-trust approach to all traffic; since data has been corrupted at scale, digital identities cannot be reliably trusted. Our platform protects all user interactions on P2P websites and apps using a combination of risk profiling and enforcement challenges.

Using a variety of digital "telltales" analyzed in real-time, the platform can accurately define between bot traffic, malicious humans and good users. This data is also supplemented with intelligence from across our vast network, meaning that fraudulent activity already spotted elsewhere will be automatically flagged before it attacks your website. Suspicious traffic is faced with a step-up authentication challenge that is near-impossible for bots to solve, and that saps the time and resources of fraudsters. Good users will rarely see it, and if they do the challenge can be solved in less than 3 seconds.

Arkose Labs further prides itself on a high level of client service. The engagement does not end after implementation. Rather it is an ongoing partnership, with a dedicated managed services team ready to help clients analyze and problem-solve any concerns that may arise and provide answers quickly.

Solution Highlights



Fraudulent profiles and listings

Prevent fraudsters from creating fake new accounts and bogus listings to defraud real users



Payments and Financial Fraud

Safeguard customers financial credentials and protect your platform from money laundering



Account Takeover

Trust is key in P2P platforms; keep your customer accounts safe from being used maliciously



Automated Spam and Abuse

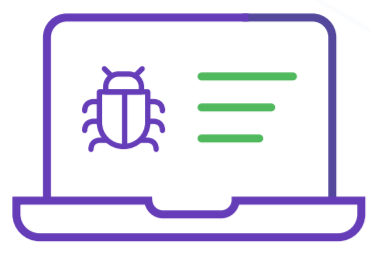
Stop bad actors from using messaging services to send malicious content



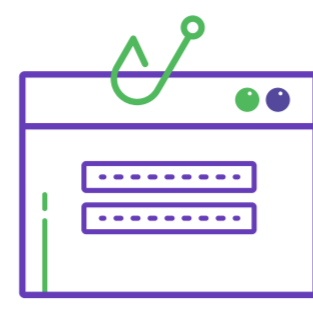
Fake Reviews

Ensure integrity of platform by preventing bogus reviews and spam upvoting/downvoting

Arkose Labs prevents fraud attacks such as:



Account takeover



New account fraud

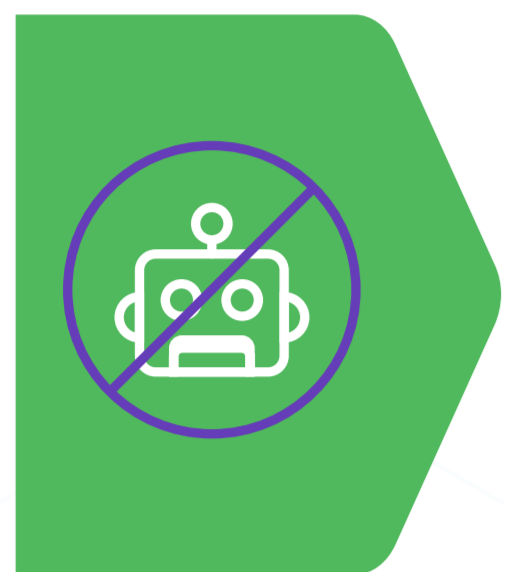


Spam & Abuse

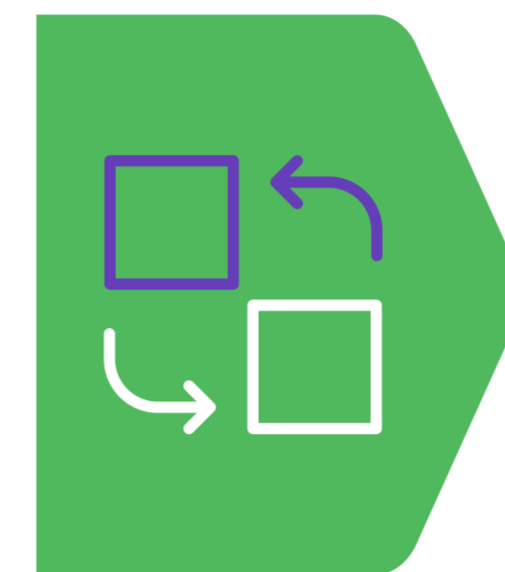


Financial Fraud

The Arkose Advantage



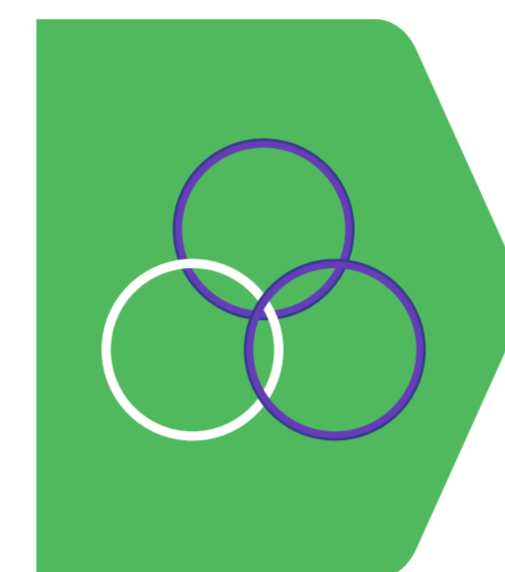
Stop Automated Traffic: Backed by a 100% commercial agreement.



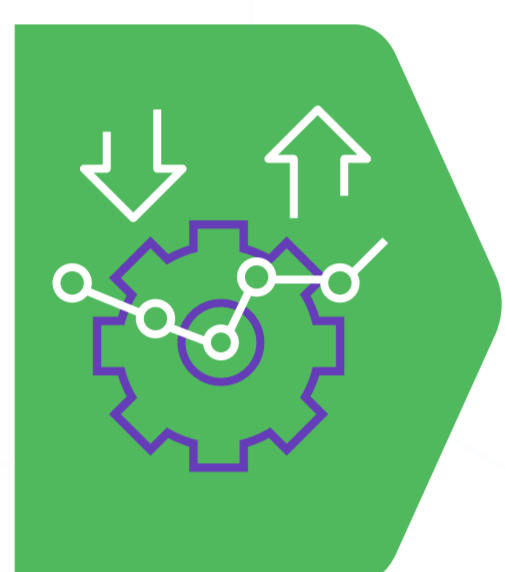
Shifts the Attack Surface: Let the bad guys attack us, not you.



Decrease False Positives: Bad traffic is challenged rather than blocked and good users have a ~98% solve rate.



Seamless Integration: Deployment can be completed in a matter of weeks, and new customers will see results within days of implementation.



Targeted Authentication: Enforcement challenges are tailored to the exact risk nature of the traffic.

Demonstrated Results

- ✓ **Slash scraping activity:** 25% improvement on legacy solutions
- ✓ **Good user throughput:** 20% increase in good traffic
- ✓ **Customer-first security:** ~98% pass rate of challenges by good users

Conclusion

Trust is the key component that makes the sharing economy financially viable; users have an implicit trust that the platforms they are using have thoroughly vetted everyone on it. Arkose Labs protects users in the digital world from all forms of online abuse, enabling you to provide a trusted platform to facilitate P2P transactions.

With precise, data-driven analysis to segment traffic, good users pass through and don't have to deal with any disruption to the seamless experience they have come to know when using digital P2P platforms. At the same time, the appropriate step-up challenges are delivered to bots or malicious human traffic, with the ultimate intent of making it economically unwise for fraudsters to attack the site. This approach stops fraud both at the point of attacks, as well as further downstream.

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.