Arkose Labs | SOLUTION BRIEF

Spam and Abuse

Protect websites and apps from malicious activity

With businesses moving online, opportunities to abuse digital properties are proliferating on a daily basis. Malicious users target every available avenue to disseminate malicious content and abuse online services for their own financial gain.

Businesses need active protection against large-scale spam and abuse to safeguard all web forms (registration, shopping cart, surveys and the like), and preserve the integrity of blogs, forums and peer reviews. They must also ensure free and freemium offerings are reserved for genuine users; protect against in-product abuse; and stamp out malicious content throughout communications channels.

Arkose Labs Solution for Spam and Abuse

The Arkose Labs platform effectively roots out automated and human-driven spam and abuse on externally facing forms and in-application customer actions.

Many organizations have deployed basic spam and abuse solutions on their websites, but are suffering due to the significant limitations of these solutions. Legacy technology cannot defend against increasingly complex attacks, and are being circumvented at scale by bots and automated solvers. The user experience is often very poor for legitimate consumers, who are presented with authentication challenges that are difficult to solve. Additionally, solutions which are designed purely to differentiate between automated and human activity cannot defend against traffic originating from low-cost human "sweatshop" resources, which are used to avoid detection by anti-bot technologies.

Arkose Labs provides a fresh approach to help drive up legitimate revenue-generating traffic on websites and apps while protecting good users from spam and online abuse. Arkose Detect provides invisible analysis of activity in real time, based on device, network and behavioral patterns. Traffic is classified and triaged based on its risk profile, flagging any telltale signals of spam or abuse. This informs Arkose Enforce, a challenge-response mechanism, which presents interactive challenges to higher-risk activity.

Technology Highlights

- **Unified solution:** Risk-based analysis backed up by secondary screening of high-risk activity.
- **Graduated risk-based friction:** Adapts the challenge to the appropriate risk profile.
- **Interactive challenges:** Root out automated attacks and sap fraudsters' time and resources.
- **In-platform protection:** Monitor and challenge user activity within the application to stop various forms of abuse.
- **Reporting dashboard:** Visibility into security across customer touchpoints.

Arkose Labs prevents spam and abuse in all its forms:

Bogus new accounts

Dissemination of malicious content

Fake reviews

In-game abuse

Romance scams

Disinformation on social media

Gift and discount voucher hacks

Scams targeting platform users

Graduated friction roots out bots of all degrees of sophistication as well as human-driven attacks. The innovative nature of the enforcement challenges ensures they are resilient to being solved automatically, as they are context-based and rendered in real time. They feature countless possible solutions - therefore automated programs cannot be trained to solve them. While good users can easily solve the puzzles to self-remediate, automated traffic fails and sweatshop traffic is slowed down dramatically. As spam and online abuse are high-volume, low-rewards activities, slowing fraudsters down ruins the potential ROI and compels them to abandon the attack.

The Arkose Advantage

Undermine the ROI of spam and abuse attacks
Targeted friction renders spam and abuse a financially non-viable attack vector.

100% SLA guarantee
Commercial guarantee that the solution protects against automated attacks of all sophistication levels.

Long-term protection
Challenges are constantly evolving and are tested to ensure resilience to machine vision technology.

User experience is front and center
Enforcement challenges are inspired by gamification, with a ~98% completion rate by good users.

Bespoke and brand integrated
Branded challenges embedded into the regular customer flow for a seamless authentication experience.

Demonstrated Results

- Increases good user throughput by 33%.
- Seven-fold increase in detecting spam and abuse.
- Lowers the instances of downstream banning of bad users.
- ~98% pass rate of challenges by good users.

Conclusion

Arkose Labs provides a flexible solution, which can protect any customer action from malicious activity. With embedded machine learning and advanced analytics, Arkose Labs provides an impressive level of sophistication to keep ahead of the evolving spam and abuse tactics, but without the complexity. The solution can be deployed and tuned within weeks, even for large and complex organizations. Its bilateral approach combines passive analysis and interactive challenges which is highly effective at deterring large-scale, malicious activity targeting digital properties.

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.

Schedule Demo

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