Arkose Labs | SOLUTION BRIEF

Scraping
Stop Malicious Web Scraping

In today's information-rich economy, malicious scraping can lead to significant financial losses for businesses, and put user information at risk. Bad actors are posing as genuine traffic in order to scrape data, content, images and commercial information, using a wide range of freely available bots and scripts. The sophistication of the programs used to scrape content is constantly improving, which enables bad actors to mimic genuine consumer behavior with greater accuracy. They are, therefore, able to circumvent traditional bot detection solutions with increasing ease.

Arkose Labs Solution for Scraping

Arkose Labs prevents scraping by eliminating malicious automated traffic and undermining the ROI driving attacks.

Arkose Labs can accurately distinguish between human and automated traffic, and stop scraping attacks from achieving scale. It classifies traffic based on its origin and intent, and presents interactive challenges to higher-risk activity.

Automated scraping tools are adept at circumventing detection by obfuscating and randomizing device, network and IP characteristics. This is why Arkose Labs takes a zero-trust approach to the data being presented. It analyzes traffic based on intent and behavior using telltale signals which point to malicious activity.

Higher risk activity is presented with secondary screening using interactive challenges. Rather than blocking activity (which may turn out to be genuine), this approach allows legitimate humans to pass with ease, but the barrier is far too high for large-scale scraping. Context-based challenges are rendered in real time with countless permutations, meaning they are guaranteed to prevent unwanted automated traffic. This undermines the ROI and renders scraping economically non-viable.

Technology Highlights

Real-time analytics. Arkose Labs analyzes traffic in real-time to determine its true intent.

Risk classification of traffic. Traffic triaged based on its risk profile and sent for secondary screening when scraping is suspected.

Graduated risk-based friction. Higher risk traffic served increasingly complex challenges.

Interactive challenges. Game design principles are used to make the challenges fun and interactive for good users that see them.

Anti-automation acid test. Definitive classification of bot versus human traffic.

Unified platform and dashboard. Easy-to-use dashboard provides multiple reports and visualizations.

Arkose Labs is highly effective at protecting against unwanted scraping activity targeting:

- Product prices
- Personal information
- Inventory
- Content
- Proprietary research

Scraping tends to be a high-volume, low-yield activity, so fraudsters use automation to achieve sufficient scale to maximize their return on investment. The scraped information can be monetized through third parties and competitors eager to acquire valuable commercial information and augment existing data sets.

The Arkose Advantage

Determines true intent of traffic. Accurately differentiate between legitimate traffic and malicious scraping.

Renders scraping unprofitable. Arkose Labs makes attackers expend time and resources to the point where it becomes unprofitable for them to continue.

100% SLA guarantee. Commercial assurance against all unwanted bot-driven traffic.

Shifts the attack surface. Bad actors attack the Arkose Labs platform, not the client's web and mobile properties.

Never blocks good users. Bad traffic is challenged rather than blocked and good users have a ~98% solve rate.

Bespoke and brand-integrated challenges. Ensures a seamless customer experience with branded challenges, which can increase good customer throughput by 5-10%.

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

Arkose Labs enables companies to protect their data and content -- the lifeblood of their business--from malicious scraping attacks. Real-time analytics segments the traffic based on its intent and bot traffic is presented with interactive puzzles. The efficacy of these challenges allows Arkose Labs to offer an industry-first 100% SLA guarantee against automated attacks.

This bilateral approach provides future-proof prevention of scraping attacks, allowing businesses to better differentiate between legitimate and malicious activity. Malicious users cannot perform scraping at sufficient scale to get any ROI from this activity. Additionally, good users are never blocked, meaning businesses protect revenue-generating traffic which helps the commercial success of the company long-term.

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.