



API Abuse

Protect APIs from bots impersonating legitimate traffic



It's the era of the "API economy" and businesses are experiencing a deluge of attacks on their web- and mobile-facing APIs. Attackers are using sophisticated programs to impersonate genuine users, emulate legitimate devices, and carry out many forms of fraud.

Attackers can target APIs to perform credential stuffing attacks, scrape content and data, set up new accounts, carry out bonus abuse, and run scripts on gaming platforms to steal in-game rewards, among other activities. They carry out large-scale attacks which put genuine users at risk and cause serious, direct losses to digital businesses.

Arkose Labs Solution for API Abuse

Arkose Labs provides powerful protection of web- and mobile-facing APIs through a combination of real-time analysis, dynamic tokens, and interactive challenges.

Protection of APIs using traditional bot detection solutions is becoming obsolete, as perpetrators can mimic genuine traffic and fly under the radar of velocity rules. Just as one can no longer rely on static identity data and passwords to authenticate users, static API keys are hard to secure and need additional verification to confirm that traffic is coming from a genuine source.

Arkose Labs uses a multi-pronged approach to protect APIs from large-scale attacks which emulate remote clients and impersonate true users.

To eliminate traffic targeting the API directly, the solution embeds an Arkose Labs token into the web application or mobile SDK, and each request dynamically verifies that the token has passed from the client to the server. Arkose Labs monitors all traffic for known signals of abuse, using behavioral fingerprints, velocity and rate monitoring, and a proprietary user IP database.

Additionally, Arkose Labs provides secondary screening of all suspicious traffic, using 3D visual challenges which are rendered in real-time and resilient to automated solvers. Bot attacks fail spontaneously when met with these interactive puzzles.

Technology Highlights



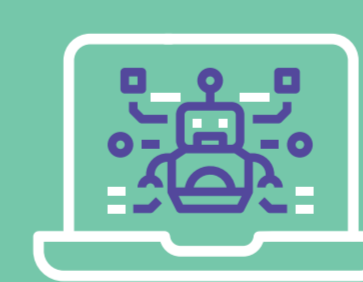
Dynamic tokens embedded in the web and mobile applications verify the legitimacy of the traffic source.



Real-time analytics provide insight into device, network, location and velocity.



Risk classification of traffic based on known telltale signals of fraud learned across a global network.



Secondary screening of high-risk traffic provides deterministic detection of bots.



Interactive challenges cause all malicious automated traffic to fail.

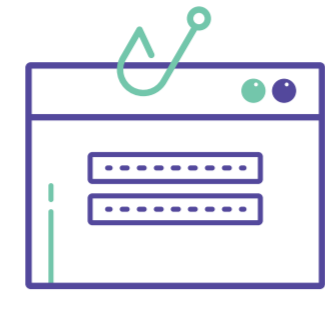


Unified platform and dashboard provide actionable insights and clear visibility into threats.

Arkose Labs prevents downstream fraud from API Abuse:



Credential stuffing



New account fraud



Bonus abuse

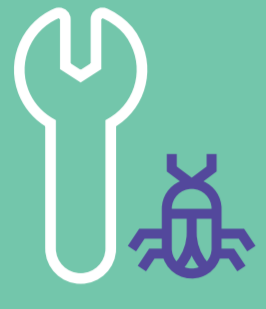


In-game abuse



Scraping

The Arkose Advantage



100% SLA guarantee:

Arkose Labs is the only vendor to provide commercial assurance of elimination of automated attacks.



Next-generation technology:

Arkose Labs goes beyond traditional bot solutions to provide multi-pronged detection and mitigation of attack.



Intent-based analysis of traffic:

Classification of traffic using a rich variety of real-time signals and behavioral indicators.



Renders attacks on APIs unprofitable:

Arkose Labs' ethos is to ensure attacks are too difficult and costly for perpetrators, compelling them to move on to easier targets.



Future-proof solution:

Protection that is resilient to the evolving sophistication of bots and automated scripts.

Conclusion

Arkose Labs combines a passive and interactive approach to eliminate illegitimate sources of traffic to APIs and prevent bots from impersonating users. A major step forward from traditional bot detection technologies, this provides long-term protection against fraud and abuse in its many forms. Guaranteed by a 100% SLA against automated attacks, businesses can have an entirely new level of confidence that the traffic they are seeing on their APIs is legitimate, addressing a major risk to the business.

**Book in your
live demo today**

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

Arkose Labs bankrupts the business model of fraud. Its patented platform combines Arkose Detect, a sophisticated risk engine, with Arkose Enforce, which uses targeted step-up challenges to wear fraudsters down and diminish their ROI. The world's largest brands trust Arkose Labs to protect their customer journey while delivering an unrivaled user experience.

© 2020 Arkose Labs. All rights reserved.

© 2020 Arkose Labs. All rights reserved.