Arkose Labs | SOLUTION BRIEF

ZeroBot

Eliminate automated attacks of all sophistication levels

It's never been easier or more inexpensive for fraudsters to launch automated attacks at scale. Bot programs that can bypass most authentication solutions are readily available on dozens of hacker websites -- and some even come with dedicated customer service.

For businesses, this means bot attacks are more prevalent than ever before and the cost required to fend off these escalating attacks has risen exponentially, thus requiring a new and innovative approach. It's imperative to deploy the most advanced bot detection to spot and avert even the most sophisticated threats, so you can stay one step ahead of the bad guys and keep automated attacks away from your business.

Arkose Labs Solution for Bot Attacks

A multi-layered approach to identify and stop bot activity.

Arkose Labs' ZeroBot solution is a holistic approach to detect and stop automated attacks. It uses a signatureless assessment that analyzes behavioral biometrics and heuristics to detect telltale signs of automation and distinguish even the most advanced bot activity from legitimate use.

This is combined with our proprietary enforcement challenge,which is rendered in real-time and designed specifically to combat the latest and most cutting edge innovations in machine vision learning. And they are generated randomly and in real time, meaning even if fraudsters spend hours of their time custom-building a bot to defeat one image, it will be immediately obsolete.

This secondary screening through challenges allows for additional analysis of behavioral, browser, and device signals for high risk traffic and compares them against legitimate human behavior over time.

This analysis is done behind the scenes during any user action on your website or within an application - without encroaching on users' privacy. The Arkose Labs platform can triage good user traffic from bot traffic with a stunningly high degree of accuracy, meaning good users rarely see these challenges. And if they do, they are simple, quick and fun to complete.

The Steps to Bot Elimination

Step One: Real-Time Traffic Analysis

- Behavioral biometrics: Pressure, keystroke, motion, swipe patterns, navigation and more
- User- analytics: Familiarity with a web page and the data and information displayed
- Network intelligence: Real-time comparison with global network of known bot indicators

Step Two: Behind the Scene Interactive Challenges

- Proof of work: Invisible to standard users, this type of test is used to prove the end-request device has certain capabilities, such as the ability to log cookies
- Proof of activity: A more advanced proof of work, where the recipient must not only show device capabilities, but perform an action as well. They are simple for real users to complete, and designed to be used in low-risk scenarios, such as where a user might pass rate limit threshold

Step Three: User-Friendly Interdiction

- Interactive 3D visual challenges that are easy for customers but hard for bot
- User behavior analysis: Behavioral biometrics and timing users completing challenges
- Anomaly detection trains the platform in real-time, with the challenge as the feedback loop

Arkose Labs prevents bot attacks such as

Account Takeover | **New Account Fraud** | **Spam** | **API Abuse** | **Scraping** | **Payments Fraud** | **Bonus Abuse**

The Arkose Advantage

Stop All Automated Attacks. Backed by a 100% commercial service level agreement.

Unified Solution. Offering both bot detection and remediation of attacks through enforcement challenges.

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

Shifts the Attack Surface. Attackers are diverted to a third party instead of attacking your site directly.

Seamless Integration. Deployment is quick and seamless, and new customers will see results within days of implementation.

Dynamic Defences: Fraud prevention that adapts to evolving attack patterns.

Demonstrated Results

Stop automated attacks
Eradicates all bot attacks against businesses

Good user throughput
20% increase in good traffic

Customer-first security
~98% pass rate of challenges by good users

Conclusion

Bot attacks are more frequent and more vicious than ever before. And with the rise of bot marketplaces, any fraudsters with a few spare dollars can afford to implement automated scripts to attack businesses relentlessly.

To defend against the varied and sophisticated automated attacks that are happening today, businesses need a multilayered bot detection and prevention solution. One that can not only accurately detect bot traffic, but stop it too. That's why ZeroBot utilizes best-in-class machine learning and analytics to power a continuously evolving risk and detection engine. Malicious automated traffic is served enforcement challenges that are specifically designed to befuddle even the most advanced bots. Arkose Labs can be your partner in stopping automated attacks for good.

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

Schedule Demo