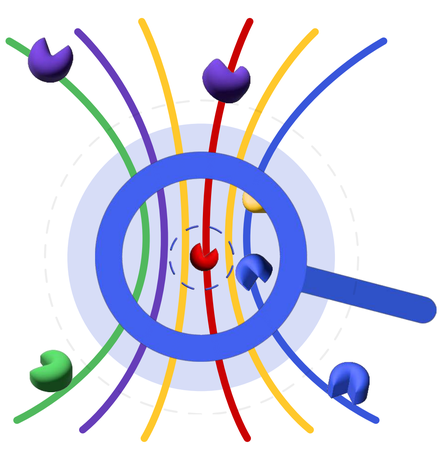
Arkose Labs

Top 10 Considerations When Looking for a CAPTCHA Vendor

The key to effectively safeguarding business platforms and keeping customers safe today is by stopping malicious bots. Unfortunately, due to rapid advancements in image recognition software, bots can easily beat traditional, legacy CAPTCHA challenges, so it's important to ensure the vendor you select can sufficiently protect you from this ever-evolving threat.
Here are 10 considerations to keep in mind when looking for a CAPTCHA vendor.

01 Be Future Proof Against the Full Range of Bot Attacks

The optimal solution should protect against not just basic bots, but even advanced, or so called "intelligent" bots. It should be "future proof" and continuously evolve in order to stay ahead of the increasing sophistication of today's bots.

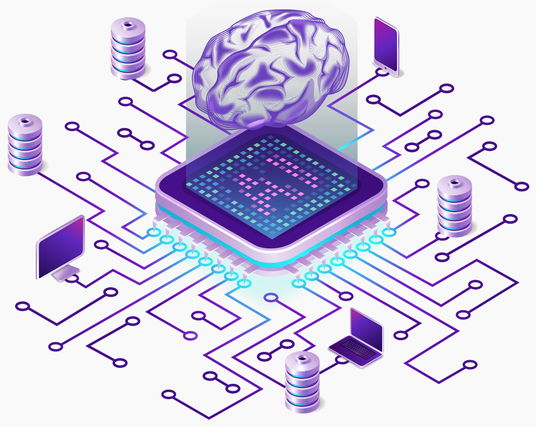


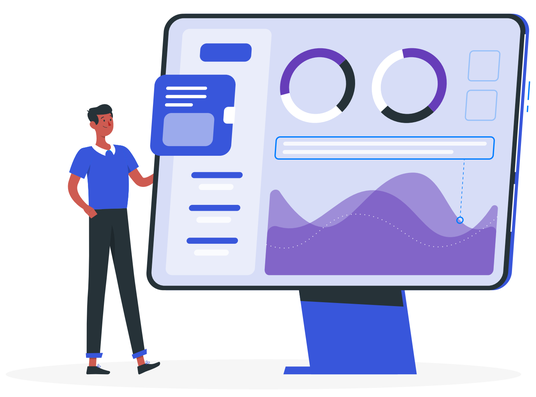
02 Robust Detection Engine

Increasingly sophisticated bots can mimic human users with a high degree of accuracy. The ideal solution should be able to accurately identify bots, differentiate between good and bad bots, identify the type of bot attack, and be able to detect even the most complex attacks. The solution should incorporate data points like global telltales (common or known bad signatures), which makes it more effective out of the box as opposed to needing time to train models.

03 Machine Learning Usage and Training

The ideal solution should deploy machine learning to identify new attacks. The vendor should ensure its data sets are sufficient and up to date for training the model, and frequently retrain the model to account for new threats, changing signatures, or customer-specific requirements. In addition, the solution should natively enable feedback loops to its client's security teams to notify them of attacks, responses, and the results of the response, and be able to push new rules to customers based on discovered threats.



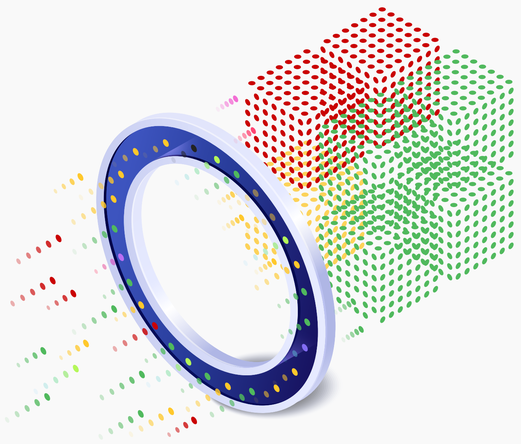


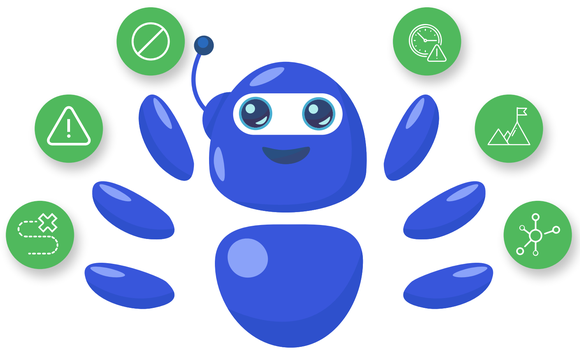
04 Explainability and Transparency

Businesses using a bot prevention solution need to know why a certain conclusion was reached. Bot defense platforms should present their clients with a risk score, bot classification, and detailed session telemetry with reason codes. Session flow diagrams should present explanations in an easy-to-consume way, with insight into bot traffic identification accuracy.

05 End-user Experience

Ultimately, how effective a solution is at stopping bad bots is meaningless if it also stops too many good users. The solution should leverage real-time signals (such as device, network, behavior), advanced ML models, and historical insights to accurately differentiate good traffic from bad.



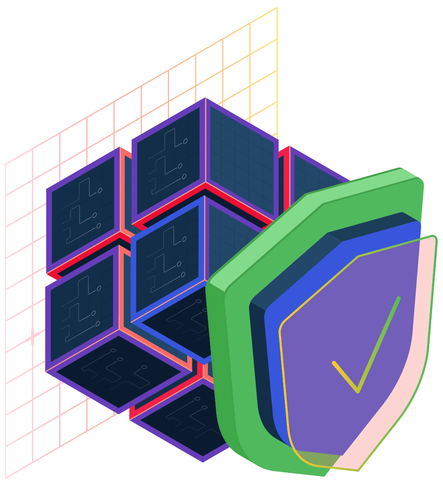


06 Efficacy of Response Types

Businesses that are the target of frequent bot-powered attacks need to consider how the solution natively responds to attacks, such as by alerting, blocking, delaying, challenging, misdirecting, or creating honeypots. Even more importantly, does it have a native challenge option to stop bad bots, or would you have to invest in another solution to provide that as well?

07 Response Configuration & Exception Handling

A bot prevention solution should not hinder or cause much friction to good users. The product should enable its customers to set exceptions for false positives or good bots. This can be done effectively by leveraging global rules, signatures, and learnings to define a custom attack response configuration to, and if needed, surgically override the set global response.



08 Privacy

Data privacy has never been more important than it is now. Consumer data privacy laws grow in number seemingly by the day, and any bot prevention vendor should make sure it is not violating data privacy regulations. Legacy captcha solutions like reCAPTCHA use cookies to determine whether a user is a bot or human. Consumers who are not Google users must share their data, which leads to data privacy concerns.

09 Set Up & Implementation

Clients should not have to spend a lot of time and effort in order to get a bot prevention solution up and running and configured to their specific needs and the customer should be able to quickly begin to see value from the bot management solution after implementation.

10 Level of Performance

The vendor should be able to ensure its product enables good performance for its customers, including low latency, high availability, and scalability across all types of endpoints. The vendor should also offer SLAs or other types of commercial assurances that its solution works as advertised. That means they stand behind their product.

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a “Cool Vendor in Fraud and Authentication”, the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput.

Schedule Demo

demo@arkoselabs.com
arkoselabs.com