kasada

WHITEPAPER

A Bot Management Checklist: 10 Must-Have Capabilities for Stopping Malicious Automation

Introduction

On average, one-third of all internet traffic is non-human. In fact, across many industries, the majority of login attempts are actually fake.

Chances are good that even if you have a current bot management solution in place, you still don't know the true percentage of non-human traffic hitting your websites, mobile apps, and APIs, and even worse, you're unable to stop the bad bots from impacting your business. That's because bots are a lucrative source of revenue for bot operators, who continue to invest in improving the sophistication of their automated attacks to avoid detection by most solutions.

Before you settle for only finding and blocking some, but not all, of the malicious automation attacking your web, mobile and API channels, consider your alternatives. Today there is a way to not only keep pace with bot operators to detect and block their attacks but also go a step further to make your online properties financially unviable for bot operators to attack.

By using the questions in this guide, you can evaluate your bot management choices to see which can help you best protect your business against automated attacks.

Every Business Needs the Right Bot Management Solution

Some bots are benign, like web crawlers, which help your websites get found. However, many are bad bots that attack your online channels take over accounts, hoard inventory, scrape data and content, test stolen credit cards, and commit other malicious and fraudulent activities.

Stopping bot attacks before they can impact your business, customers, shareholders, and bottom line requires a different approach than traditional solutions, one that helps you win the battle against malicious automation.

Given the growing marketplace (and hype) for bot management solutions, how can you know what to look for and which capabilities are most important for solving online traffic integrity problems? The following pragmatic questions can help you get the answers you need to make the right decision.

The Top Ten Questions to Ask Bot Management Vendors

Question 1:
Does your solution address the fundamental financial driver of automated attacks?

Simply blocking an attack doesn't make the attacker go away. That's because bot operators are primarily motivated by financial gain and know that to achieve their goals, they simply need to adjust their techniques until they evade your defenses.

Kasada turns the tables on attackers by providing the bot with increasingly difficult cryptographic, proof-of-work challenges that exhaust the compute resources of the automated attacks (and the wallet of the bot operator). It makes any continued attempts at attacking your business financially unviable for bot operators, removing their motive for attack and forcing them to move on to easier targets.

Question 2:
Can your solution detect evolving bot attacks?

Many solutions rely primarily on data from the past to detect bot attacks. Because bot operators constantly revise their methods to evade detection, these rule-based solutions are always a step behind. Many vendors state that they can stop 99% of bad bot requests, but that's not enough. For a bot operator, a 1% success rate for a bot launching 100,000 attacks an hour equates to 24,000 successful account breaches a day.

Kasada's unique sensor detection and inspection approach identifies and blocks attacks without having to rely on known behaviors and IP addresses. Our threat research, combined with real-time request analysis, reveals patterns in bot behavior. Correlating telemetry data collected by our sensors, our inference engine can decide whether the client is human or automation.

Question 3:
Can your solution stop attacks at the first request before accounts are breached or other damage is inflicted?

Most solutions cannot detect automated attacks before the page loads because of the way the bot management software is architected. Such solutions can't detect content scraping, for example, before it happens.

Kasada takes a different approach. When bots imitating human users interact with your application, they leave certain traces of themselves within the client environment. Kasada's invisible client interrogation process detects the presence of such traces and uses the telemetry in our decision engine to detect and stop attacks. Kasada looks for immutable evidence of automation from the very first request with extremely low false-positive rates and long term efficacy. It is also able to detect and block scraping attempts before they inflict damage.

Blocking scraping attempts before the page load completes further reduces load on your origin server resulting in significant savings for your company as well as improved performance.

Question 4:
Can bot operators reverse-engineer your solution to allow their bots to evade detection?

Many attackers retool their automation based on what they discover about the methods used to detect them and thwart attacks. The more they can learn about the bot management solution you're using, the easier it is for them to iterate on their automation to stay ahead of you.

To achieve efficacy over the long term, a bot management solution should aim for very slow, arduous, and confusing feedback cycles so that bot operators give up and move on to easier prey. Most bot management vendors don't protect the data they collect; it's in the open for attackers to read. Some don't even obfuscate their code.

Kasada's bot detection process is distributed and dynamically obfuscated behind your content delivery network (CDN) in a way that makes it almost impossible for fraudsters to reverse-engineer and then develop workarounds for it. Kasada also keeps the feedback signal to attackers very low using creative responses, obfuscates sensor code (both web JS and mobile SDKs), encrypts sensor data, and continuously changes sensors, via feedback cycles from our Threat Research team.

Question 5:
Can your solution be deployed and also demonstrate value within minutes?

Most solutions on the market today are complex to deploy, configure, and operate, requiring you to continuously manage and update them to realize ongoing value and improve long-term efficacy.

Kasada is the fastest bot mitigation solution to implement, with the fastest time-to-value. Your team can start seeing value within 30 minutes by immediately neutralizing the impact of automated attacks on web, mobile apps, and APIs. With Kasada, you can dramatically reduce the human time associated with managing bots, freeing your staff to work on other high-value efforts.

Question 6:
Will your solution provide visibility into human traffic and analytics to help optimize marketing?

The open secret in bot management is that vendors readily generate reports of what they detected and blocked, leading you to assume that the remaining traffic must be benign— nothing to investigate. It's not in their best interest to give you the tools to carefully investigate the remaining traffic because you might notice attacks that the software missed.

Question 7:
Does your solution protect APIs, too?

APIs are a favorite target for attacks because the number of APIs have increased faster than IT can keep track of them and secure them. In fact, Gartner predicts that API abuses will become the most-frequent attack vector by 2022.[1] Consider the damage that automated attacks—such as those attempting login and credential abuse—can have on your authentication endpoints.

Kasada API protects an organization's web and mobile APIs from automated attacks, botnets, and targeted fraud. Together, Kasada Web and Kasada API offer seamless protection across all of your web properties, mobile apps, and APIs, detecting and blocking automated attacks.

Question 8:
Can your solution block attacks without impacting our real users?

Solutions based on historical and contextual data, such as IP addresses and analysis of known behaviors, often block and blacklist IP addresses with poor results, often to the detriment of the user experience. Alternatively, relying on CAPTCHA challenges are not only ineffective at detecting and stopping automated attacks, but they too deliver a terrible user experience, frustrating your customers from using your web properties and leading to lower conversion rates.

Kasada uses dynamic methods, invisible to end users, to detect automation with unprecedented accuracy. We architected the solution to create an invisible process that does not rely on CAPTCHAs, instead delivering a frictionless experience for customers. In fact, Kasada reduces latency by suppressing synthetic traffic, which can significantly improve and optimize the user experience.

Question 9:
Is your solution easy to operate and manage?

Many bot management vendors require significant code changes to integrate their solution into your environment. Others have an extremely complex configuration model that is time-consuming to tune to maintain and improve effectiveness.

Because of that challenge, it is common for bot management solutions to need two full-time security professionals dedicated to ongoing tuning and maintenance or to pay for a managed service.

Kasada is a cloud-based service that easily implements within minutes and offers an embedded, immersive 24/7 customer support via an "always on" chat channel, putting no extra maintenance burden on your internal team. With Kasada, you can easily expand protection to new websites, mobile apps, and APIs. It doesn't require extensive maintenance and tuning (or personnel) to achieve long-term efficacy against evolving threats.

Question 10:
Is your solution CDN-agnostic?

It's important to choose a bot management solution that doesn't lock you into a single content delivery network (CDN) provider. This is important for companies using multiple CDNs to deliver their online traffic. They need a single solution that can protect all of their digital properties regardless of CDN being used.

Kasada is CDN-agnostic, giving you the flexibility to change your CDN, if needed, in the future, and protect all of your digital properties regardless of which CDN you're using.

[1] "What You Need to Know About the New OWASP API Security Top 10 List," Maria Korolov, CSO, November 2019.

About Kasada

Kasada is the most effective and easiest way to defend against bot attacks across web, mobile, and API channels. Its modern, proactive approach adapts as fast as the attackers working against them. The solution frustrates and strikes back at fraudsters to make automated attacks unviable. Invisible defenses eliminate the need for CAPTCHAs and ensure a frictionless user experience. Kasada onboards customers in minutes, requires no ongoing management, and empowers enterprises with long-lasting protection and optimal online visibility. Kasada is based in New York and Sydney, with offices in Melbourne, San Francisco, and London. For more information, please follow us on Twitter, LinkedIn, and Facebook and visit www.kasada.io.