



The Top 10 Considerations for Bot Management

ebook



TABLE OF CONTENTS

Introduction	03
1. Sophisticated expertise	04
2. Intelligence	05
3. Resilient protection	06
4. False positives and false negatives	07
5. Flexible actions	08
6. Deployment	09
7. Visibility and reporting	10
8. Protecting APIs	11
9. Site vs. page	12
10. Managed services	13

Introduction

Wondering how difficult the problem of bots has become? Try to score a Taylor Swift ticket or a new pair of Air Jordans. And those are just hype events. Bots are becoming increasingly pervasive and pernicious across industries.

What's worse for those looking for answers is that the bot management game has changed. Truthfully, it has always been changing. Bot management is often described as an arms race, or a game of cat and mouse, with businesses erecting defenses and bot creators continuing to find ways around them. But now it's not only the bots themselves that are evolving. The environment around them is evolving as well. For example, businesses are no longer dealing just with individual actors, or even coordinated groups. It is now possible to rent a bot for the week, like you would an Airbnb. Similarly, solutions cannot just segment bots into categories of good and bad. There's too much of a gray area now.

This evolution of bots and the environment around them has made the task of selecting bot management software more difficult than ever. You need to not only determine what was effective against yesterday's bots, but what will be effective against today's and tomorrow's.

This guide outlines some of the key considerations for buyers selecting bot management software. Use it to help you sort through the noise to make an informed buying decision.

1 Sophisticated expertise

Bot management solutions, by definition, detect bots. In other words, they're looking for signs of automation and other indicators that the requestor isn't a human. However, as bots have evolved and become more sophisticated, they've also become more specialized. Bots are now designed for targeted purposes such as scraping content from your site, hoarding your inventory during hype events, and credential stuffing to take over your customer accounts, among other use cases. And often detections for one kind of specialized bot won't detect the others. You need to know if the vendor can stop the specific bots you're facing, not just the basic, general-purpose bots.

Considerations:

- Does the vendor have specialized detections for bots based on business use cases?
- Can the vendor demonstrate its expertise in the specific bot problem you have?
- How many of the vendor's other customers are facing the same issues? Will you benefit from what the vendor has learned from those customers?
- Does the provider offer reports, services, or other capabilities to further support your battle against specialized, adversarial bots?



2 Intelligence

A bot management solution is only as good as its ability to recognize the characteristics of the bots it's monitoring. While some vendors may claim to detect 99.9% of bots, it's impossible to objectively measure effectiveness. Bots are always changing, so what you caught yesterday probably learned how to evade that detection today. A better criterion for evaluating bot management tools is how the vendor informs its bot detection capabilities. You need a solution that can detect the most sophisticated bots (not just the usual suspects) and one that pulls from the largest dataset. Keep in mind that many artificial intelligence (AI) and machine learning (ML) tools are open source, so the amount of data, cleanliness of the data, and the speed with which the solution feeds the data to the algorithms is an underappreciated consideration when evaluating a solution's AI/ML. The insights should include trust indicators and risk scores across every login, across domains. Additionally, effective solutions should take a multipronged approach to bot detection, using the latest methods.

Considerations:

- Ask for details on how the vendor informs its bot detection capabilities. Vendors with large customers that are attractive to attackers are going to have more experience and more comprehensive datasets on which to build their capabilities, including which risk and trust signals to evaluate, more device anomaly detections, among others. A lack of transparency should be a warning.
- Does the vendor use AI/ML to support the solution? How sophisticated are those models? And just as important: How much data does the vendor feed into those models? Attackers are certainly using AI. You should be too.
- AI is not enough, however. Does the vendor have a team of qualified experts like security researchers and threat intelligence analysts who constantly look for novel attack techniques and monitor hacker communities to ensure you're always a step ahead?



3 Resilient protection

When you block a sophisticated bot, it doesn't go away permanently. It keeps coming back, constantly mutating in an attempt to evade your detections. Many bot management solutions can detect the bots (or at least some of them) initially, but then lose effectiveness once the bots start mutating. Akamai has seen bots mutate in a matter of hours. Traditional development cycles are too slow to keep up. Make sure the solution you select learns and evolves over time, preferably using machine learning automatically. That should include preemptive defenses that make it harder on attackers who seek to gain information they will use to evade your defenses.

Considerations:

- Look for a solution with the most sophisticated bot detection technologies (like user behavior analysis and customer-specific learning models). These will remain effective longer as the bots mutate.
- Find out if the solution includes defensive tactics like JavaScript obfuscation, which makes it harder for attackers to reverse engineer bots that can sneak by your defenses.
- Ask for proof or references from other customers who have deployed the solution to see if it has remained effective over time.



4 False positives and false negatives

When a bot management solution shows it has blocked a bot, how do you know that the system didn't actually block a legitimate user? Many vendors play fast and loose with false positives. If they lack a solution that scores bots against every detection, they may not be able to detect gray bots, leading to binary yes/no decisions. And often, those vendors like to show customers that they blocked lots of "bots," even if their false positive rate is high, meaning they're stopping bots but also valid traffic – humans or "good" bots that are valuable to your company. On the other hand, a low false negative rate sounds great until you realize that the false negative rate is so low because the vendor had to reduce the overall solution effectiveness to make sure it wasn't blocking human users – and then winds up letting bots through that it shouldn't. You want to block malicious bots without getting in the way of your business, but you also don't want to lower your protection. You need to have confidence that the vendor you're partnering with cares about accuracy and the impact of false positives and false negatives.

Considerations:

- Does the vendor leave it up to you to tune for false positives/negatives, or does it invest in capabilities and services to work collaboratively with you?
- Does the solution learn from traffic patterns across sites and autotune itself to reduce the burden on your team?
- Does the vendor suggest using a CAPTCHA instead of other challenge actions? That's often a dead giveaway. Users hate them, but it's easier for a vendor to offer a CAPTCHA than to tune its rules to minimize false positives.
- Do you have visibility into why the solution flagged a request as coming from a bot? Or is it a black box? Look for the ability to verify actions taken with granular visibility into requests and the ability to visualize changes in your settings before you put them into production.



5 Flexible actions

It's tempting to think you only need to worry about blocking bad bots while letting good ones through. But the environment has become much more complex than that. Many bot operators have learned how to lower their risk signals enough to put their bots in a gray area, knowing most organizations would rather risk letting in a bad bot than risk blocking a legitimate user. Your solution should provide a set of sophisticated actions so you can go beyond block or allow to include challenge actions like cryptographic challenges and step-up MFA. And your solution should also include actions for dealing with other kinds of situations, like with good bots. You might want to slow down your partner bots during heavy traffic times and let those bots through immediately during off-peak times. You can also choose different actions for bots in the same known category — for example, if you're a retailer, you can let the more popular coupon bots check your site while blocking ones you don't want to do business with. You need the flexibility to apply different actions on different types of bots based on their impact to business and IT — especially when that varies based on location, time of day, or seasonality. More than that, you'll need a solution that doesn't simply block all bots (and, by doing so, teach them to change evasion tactics) but one that creates roadblocks instead, making it more difficult and more expensive for attackers.

Considerations:

- Does the solution allow you to create different categories for different types of bots, or is it just good and bad? Can it also create different actions for bots in the same category, like search engines or financial aggregators?
- What types of conditional actions does the solution support? Does it support advanced actions — like slow and serve alternate content — that help you better shape your traffic? Does it include actions like a cryptographic challenge?
- How flexible is the solution in managing the different bots that you see? Is it just another hammer, or can it surgically apply actions based on the time of day, by percentage of traffic, or by URL?
- Can the solution insert resource-intensive problems that make it more expensive for bot operators and slow down high-request volume attacks beyond just a hard 403?



6 Deployment

When it comes to any bot management solution, how long it takes to launch the solution and how quickly you can modify it should be core considerations. Buyers should be wary of any solution that requires modification to their existing applications or impacts application performance. Deployment delays can be costly – and if you need to make changes to your applications anytime business events require it, like flash sales, that's only going to demand more resources.

Considerations:

- Does the solution work in real time without impacting the performance of your existing applications?
- Does it require you to make changes to your existing applications?
- Can it scale up or down to accommodate unforeseen events like volumetric attacks or expected events like flash sales?



7 Visibility and reporting

Every bot management solution can show you high-level statistics on your bot traffic, but you need more than that. For infrastructure planning or reporting up your management chain, high-level statistics are great, but don't provide the granularity you need to analyze your bot traffic. They also don't provide you with the evidence you need to trust that the solution took the right actions. With a solution that can block your users, you don't want a black box. You need the detailed reporting to support your business and help you better understand how changes to risk thresholds impact performance.

Considerations:

- Does the solution provide reporting capabilities that allow you to zoom in on specific bots, botnets, or bot characteristics? Can it report on different scoring segments, which bots are attacking which endpoints, and show what actions were taken?
- Can you investigate spikes in traffic and look at individual requests? Sometimes you need to see request details to know what to do.
- Can the solution show you how your bot traffic compares with others in the industry?
- How does the reporting tie in with that of other security solutions? Can you analyze your traffic holistically, or are there separate views?



8 Protecting APIs

Regardless of vendor or solution, the more sophisticated bot detection technologies today rely on injecting JavaScript code and analyzing the client response. But what do you do with your APIs when API-based clients don't respond to JavaScript? If you need to expose APIs to support mobile apps or other third parties, you need a solution that can help you protect them in the same way it protects your web pages. Otherwise, your bots (and your bot problems) will simply migrate from your web pages to your APIs.

Considerations:

- What kind of protections does the vendor provide for APIs? Is it just quota management and rate limiting?
- Look for a mobile capability that can incorporate the vendor's most sophisticated bot detections into your mobile apps.
- Although not always as effective as other active detections, a reputation-based approach may be a good option for protecting APIs that support third parties, which may not have access to a mobile capability like an SDK.



9 Site vs. page

If your website is more than a single page, you likely suffer from multiple bot problems, each affecting different parts of your site. Price scraping can have a big impact on your product pages. Content scraping can undermine your value-added digital content. Meanwhile, credential abuse attacks against your login pages are still happening. But when it comes to bot management solutions, some are designed only to address a single problem. Make sure that your management solution can help you address all your bot problems, whether they affect your entire site or only specific pages.

Considerations:

- What does the solution focus on – individual pages or the entire website?
How does it deploy – in front of individual pages or the entire website?
- Can the solution help you address all your bot problems, whether they're credential abuse, web scraping, or content aggregation?





10 Managed services

You need to manage the bots to control their impact on you and your business, but bot management isn't easy. And while you may have expertise in your company, sometimes you need extra help – you need experts who understand your bot problems. What's more, staffing these positions is becoming increasingly difficult. What happens when some of your talent leaves? Anybody can look at an HTTP request and create a signature to block traffic, but that doesn't address your problem. What you need is someone who can connect the bots back to your core problems, and design and implement a strategy to address those problems.

Considerations:

- Do you have the in-house bot-specific expertise required to get the most out of any solution?
- Does the bot management vendor offer professional services, or does it just sell products?
- Can you access proactive monitoring and supplemental expert resources in the event of an emergency at any time?





Be proactive, not reactive

You're better served by investing in bot management before bots become a problem and before the next wave of evolution renders existing defenses a weak imitation of their former selves. Take these considerations into account as you research your options. Akamai Bot Manager can help to provide the assurances you need. To learn more, request a personalized walk-through of a simulated attack.

[Learn more](#)



Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on [Twitter](#) and [LinkedIn](#). Published 09/23