NETACEA

How to Pick the Right Bot Management Solution for Your Business

INTRODUCTION

Any business reliant on online platforms needs a robust, reliable and effective solution to mitigate the risks of unchecked automated threats.

In such a diverse marketplace, selecting the most appropriate bot management solution both from a technical and business viewpoint is not a straightforward task. This guide aims to provide the right questions to ask when making your shortlist.

NETACEA

ROUNDUP:
Ten Questions You Must Ask Before Buying a Bot Management Solution

1. Detection capability: "Can your solution detect sophisticated and targeted attacks?"
2. False positives: "How accurate is the solution at correctly identifying bots?"
3. Relevancy: "Can your solution stop automated threats specific to my business?"
4. Continual analysis: "Is my traffic being continually analysed in real-time?"
5. Implementation: "Does your solution rely on client-side JavaScript?"
6. Flexibility: "Will you work with our business to develop a bespoke solution?"
7. Support: "Is responsive, fully-featured support included in the price?"
8. Pricing: "Is your pricing up-front and all-inclusive?"
9. Expertise: "Will I have access to the latest insights and technology?"
10. Reputation: "Is the solution proven in your market?"

Next step: Complete our checklist before you decide which bot management solution to purchase

DETECTION CAPABILITY:
“Can your solution detect sophisticated and targeted attacks?”

In recent years we have seen rapid advancements in the sophistication of bot attacks. Bots can bypass rate limiting, avoid JavaScript detection and distribute across proxy networks with ease.

What should I look for?

To be effective, it is essential for a bot management solution to use a range of techniques and data points to detect bots and stop these attacks.

What am I getting?

Without conducting a proof-of-concept with a solution, it is impossible to know how effective it is at uncovering the myriad of bots targeting your organisation.

NETACEA

FALSE POSITIVES:
“How accurate is the solution at correctly identifying bots?”

A “false positive” occurs when a real human user is misidentified as a bot and denied access to the website or application based on this incorrect categorisation. In many cases, false positives can cause even more commercial damage than bots themselves.

Taking online retail as an example, incorrectly labelling a real customer as a bot costs the business a potential sale and delivers a poor experience to that genuine user. Because visitors are frequently grouped together based on demographics, it is common for large batches of users to be misidentified in this way, compounding the issue.

In past incidents, a high false positive rate in bot detection has caused significant loss in revenue, brand damage and broken trust with actual consumers.

What should I look for?

Bot management providers should be open about false positive rates. The lower this figure, the fewer false positives the bot management solution will generate and the less risk there is of the solution negatively impacting your business. A good rate is anything below 0.001%.

NETACEA

RELEVANCY:
“Can your solution stop automated threats specific to my business?”

Because each solution uses different methods and technologies to detect bot traffic, some are better suited to rooting out certain types of bot traffic than others. For example, one solution might excel at detecting scraper bots, however if your business is more susceptible to credential stuffing, you must ensure the solution is able to accurately identify bots signalling intent to carry out such an attack.

What should I look for?

Based on factors such as your business sector, size and technology, you should have an indication of the kind of bots likely to have the most impact, whether that’s scalpers, scrapers or credential stuffers. It is vital to identify these early and find out whether your bot management vendor can evidence their ability to tackle these specific bot threats.

What am I getting?

By conducting a proof of concept, the bot management solution should be able to identify not just the presence of bots, but also their intent and methods of attack.

CONTINUAL ANALYSIS:
“Is my traffic being continually analysed in real-time?”

Some bot management solutions challenge suspicious users on first entry, using cookies to mark visitors as bot or human so the system can react accordingly on future visits. However, there is now an online market for genuine user cookies, which are bought wholesale by bot operators to circumvent this type of bot detection.

What should I look for?

AI based bot detection technology does not rely on a simple block list to categorise bots and humans. Although bots act like humans to achieve their objectives, there are still behavioural signals of them not being human. Therefore, it is vital to continually assess the behaviour of each user in real-time to detect non-human activity and take appropriate action each time.

What am I getting?

Ask your vendor whether their solution continually monitors all users with AI or relies on adding groups of users to a block list.

IMPLEMENTATION:
"Does your solution rely heavily on client-side JavaScript?"

Many bot management solutions use JavaScript to monitor web traffic and distinguish between humans and bots. However, JavaScript-dependent bot management is becoming less useful and relevant, for several reasons:

1. ### Bots can bypass JavaScript fingerprinting
   Deploying detection criteria into the front-end using JavaScript leaves it vulnerable to hackers and bot operators to deobfuscate and build work arounds.

2. ### JavaScript must be constantly maintained by the customer
   The need to continually update solutions to keep pace with evolving threats results in additional code for you to maintain and puts live implementations at risk of falling out-of-date or becoming insecure.

3. ### Major browsers are phasing out fingerprinting
   Because third party cookies are scrutinised by privacy advocates and are a notorious attack vector within cybersecurity, they are being phased out by Chrome, Safari and Firefox.

4. ### No API coverage
   Bots are increasingly targeting native APIs, which many bot management solutions have no visibility of because of their reliance on JavaScript and mobile SDKs.

What should I look for?

Ask your vendor to confirm how their bot management solution is implemented and that it does not rely on JavaScript.

What am I getting?

Rather than using JavaScript and SDKs, server-side solutions are implemented via cloud, CDN or API. This gives full visibility of web, mobile and API traffic, and is maintained by the vendor meaning customers will always automatically have the latest protection.

Also, as server-side bot management does not expose code to the client, bot operators have no visibility of bot identification methods and cannot reverse engineer a way around the solution.

FLEXIBILITY:
“Will you work with our business to develop a solution that works for us?”

Some bot management solutions claim to be able to start blocking bots almost instantly. However, a "bad bot" for one business may be a "good bot" that generates revenue for another business. This means that a one-size-fits-all approach risks missing bot traffic or creating dangerous false positives.

A number of solutions rely on a large user base to make generalisations about vulnerabilities across industries. While useful for known large scale attacks, this approach ignores the fact that bot attacks are often heavily targeted to individual sites and can quickly adapt to expose unique business logic exploits.

What should I look for?

Only by working closely with you to understand your business, your technology and your traffic can your bot management vendor provide a solution that offers the most effective protection possible. A direct line to your bot management solution support team is invaluable, allowing for flexibility and adaptability without delay.

What am I getting?

Ask for a roadmap of engagement with your vendor, from discovery and proof of concept through to go-live and beyond. If they do not envision your bot management strategy becoming more refined and effective over time, or do not offer regular analysis with their data science team, your defence against bad bots is likely to get worse rather than better in the long term.

NETACEA

SUPPORT:
“Is responsive, fully-featured support included in the price?”

In the fight against bots it's key to have a partner to help you deal with ever evolving attacks. Many bot management solutions do not include dedicated bot management support as standard, leaving customers to fend for themselves or pay a premium price for a support package.

What should I look for?

A good understanding of your business is vital to accurate bot detection, so it is important for fully featured support to be included. You are also more likely to get better support around bot management from a vendor focused solely on bot detection and mitigation, rather than those that form part of a larger security package.

What am I getting?

For a solution as important as bot management, support should be fast, helpful and tailored to your needs as standard. Ensure the price you pay includes excellent support, verified by existing customers.

NETACEA

PRICING: “Is your pricing up-front and all-inclusive?”

Because pricing levels across the bot management marketplace vary greatly, many businesses unsurprisingly find it daunting to unravel what is included in the price they are given, and the extra charges they might expect (or not expect) to pay.

What should I look for?

Look for a simple and straightforward pricing structure, with no hidden extras for overages or inflated prices on long term commitments.

What am I getting?

Any quote should be bespoke to your needs, include everything needed to provide full protection, and be clear and up-front.

EXPERTISE:
“Will I have access to the latest insights and technology?”

As bot management has become a crucial component in a security stack, many vendors have bought up or bolted on solutions to their existing packages to tick the bot management box for existing clients. But because automated threats are evolving so rapidly and the potential impacts on businesses are so great, dedicated research is required just to keep pace.

What should I look for?

Leading bot management solution providers have dedicated data science and threat research divisions on the front line of fighting automated threats. This activity should be closely tied to product development and ongoing support with customers, ensuring that emerging bot attacks are mitigated, and expertise given where needed.

What am I getting?

Find out whether your bot management vendor has a dedicated research function. Ask about their credentials and quality of their output, and how this shapes your protection.

REPUTATION: "Is the solution proven in your market?"

Bot management is rightly a significant investment. Since such an investment aims to protect your business's reputation, you should engage with a vendor confident in their own reputation.

What should I look for?

Ultimately your chosen solution must be able to show that it will be effective in detecting and mitigating the bot threats most likely to damage your business.

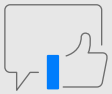
What am I getting?

The best way to know whether a bot management solution can deliver as promised is by completing a proof of concept on your website and applications. This way you can evidence the potential value the solution could deliver.

Also, seek honest feedback from current or former clients of each solution you assess about all the points raised in this guide. Look for awards and industry accolades won by the vendor that indicate third-party validation.

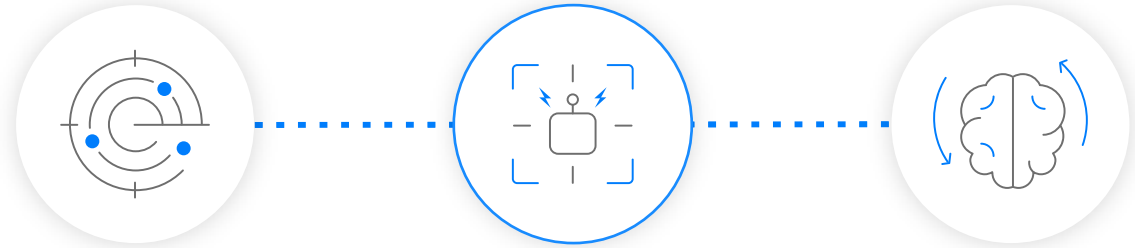
CHECKLIST:
The Core Functions and Features of Any Bot Management Solution

Before you decide which bot management solution to purchase, make sure that your chosen vendor:

-  Has demonstrated highly accurate bot detection on your own website ☐
-  Is configured and tailored to your business rather than “out-of-the-box” ☐
-  Has evidenced expertise in handling threats relevant to your business ☐
-  Includes a full support package in the price ☐
-  Has proven that they have a very low false positive rate ☐
-  Has simple and straightforward pricing ☐
-  Can verify that all user behaviour is analysed and acted upon in real-time ☐
-  Uses an approach that is backed up by industry-leading research from experts in the field ☐
-  Is implemented on the server-side, and is not reliant on JavaScript ☐
-  Can evidence an excellent reputation in the industry with recognised accolades ☐

CHOOSING THE RIGHT BOT MANAGEMENT SOLUTION

Choosing the right bot management solution is a major decision for any business. Throughout this guide we have discussed the essential requirements for a bot management solution to provide adequate protection against bot threats. This has included not only technological considerations but also the vendor's overall approach to research, development, customer service and pricing.



DETECT MALICIOUS BOTS

RESPOND TO ATTACKS

EVOLVE AND ADAPT

At Netacea we take a consultative approach, working closely with you to understand not only the threats bots pose to your business, but how our solution fits into your wider strategy and organisation.

This partnership, paired with our server-side approach and innovative Intent Analytics technology, allows us to seamlessly integrate with your business and deliver accurate, intelligent and effective bot mitigation.

To find out more about Netacea's unique approach to stopping sophisticated bot threats, visit www.netacea.com/why-netacea or talk to our team today at hello@netacea.com.

- / Real-time analysis powered by Intent Analytics™
- / Best-of-breed anomaly detection
- / Threat intelligence feed
- / Insightful, data-rich dashboards
- / Total control over response options
- / Seamless and flexible integrations
- / Dedicated bot experts with 24/7 support