NETACEA

GUIDE

The Bot Management Buyer's Guide 2023

Netacea @Netacea_AI netacea.com hello@netacea.com

NETACEA

Introduction

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

It's also important to work in partnership with your chosen vendor. You are not just buying a tool – you are buying expertise and insights into how bots affect your business. With the right bot management vendor on your side, the value of this reaches multiple business stakeholders.

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

11 Questions You Must Ask Before Buying a Bot Management Solution

1. Detection capability: "Can your solution detect both broad and targeted attacks?"
2. False positives: "How accurately can your solution identify bots and their intent?"
3. Reporting: "Does your solution provide clear and detailed information about each attack?"
4. Adaptability: "Can your machine learning models adjust to stop new attacks?"
5. Robustness: "Can motivated attackers bypass the solution?"
6. Implementation: "Does your solution integrate easily with our existing technology stack?"
7. Flexibility: "Will you work with our business to develop a bespoke solution?"
8. Support: "Is responsive, fully-featured support included in the price?"
9. Pricing: "Is your pricing up-front and all-inclusive?"
10. Expertise: "Will I have access to the latest insights and technology?"
11. Reputation: "Is the solution proven in your market?"

Detection capability: "Can your solution detect both broad and targeted attacks?"

Whilst many attackers use bots to scale up attacks across multiple targets with ease, we have increasingly seen adversaries use sophisticated bots to launch targeted attacks with alarming precision. These attacks are often the hardest to detect – and the most damaging.

It's vital to identify which kind of attacks are likely to target your business and ensure your bot management solution can detect and stop those attack types effectively. For example, any site with a login page is almost certainly under siege from credential stuffing bots, whilst eCommerce businesses are most likely the target of scalpers; your choice of vendor should be able to prove efficacy in relevant areas.

What should I look for?

Your bot management solution should use a 'defense in depth' approach, using a combination of tailored machine learning algorithms, continually up-to-date block lists of known adversaries, and intervention from bot experts, to catch both broad and targeted attacks relevant to your business.

The best way to test detection capability is through a proof-of-concept exercise, particularly if done in parallel with existing or competing tools to see which attacks were previously missed. Bot management solutions should be able to identify not just the presence of bots, but also their intent and methods of attack.

False positives: "How accurately can your solution correctly identify bots and their intent?"

A 'false positive' occurs when a genuine human user is misidentified as a bot and denied access to a site based on this incorrect categorization. Taking online retail as an example, incorrectly labelling a real customer as a bot costs the business a potential sale and delivers a poor user experience.

As bot management solutions often group visitors together based on demographics, it is common for large batches of users to be misidentified in this way, causing significant loss in revenue, brand damage, and broken trust with actual consumers. False positives can quickly cause even more commercial damage than bots themselves.

Within solutions with less accurate detection capabilities, there is a constant balancing act between blocking too much (generating false positives) and not blocking enough (letting bad bots through). The gold standard is accurate detection that blocks only unwanted traffic without needing to tweak settings ad hoc.

What should I look for?

Bot management providers should be transparent 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 and customers. A good rate is 0.001% or lower.

Reporting: "Does your solution provide clear and detailed information about each attack?"

As bot management tools need to feed information into an increasing number of stakeholders (from fraud teams to security teams, as well as operations and even marketing), clear and useful reporting is one of their most valuable features.

With detailed insights on site interactions (both benign and malicious) at your fingertips, your business can take steps to strengthen your security against known threats, and even improve user experience – with access to the right data.

What should I look for?

Different stakeholders may be short on time and only need a surface level view of attacks and mitigation activity, shown in a clear and immediately comprehensible format. Others may gain valuable insights by drilling deeper into the findings.

It's therefore key to look for a solution with the ability to dig into the data. You should be able to look at individual attacks so that you can see where they originated, their intent, their tactics, what was done to stop them and how quickly this happened.

Adaptability: "Can your machine learning models adjust to stop new attacks?"

Most modern bot management solutions use machine learning technology to identify bots by detecting known bot characteristics or behaviors automatically.

However, bots are constantly changing their tactics or even developing brand new attacks that require more adaptable machine learning approaches to detect. A 'defense in depth' approach using different types of machine learning models to fit each attack type is needed to stay ahead of bots as they evolve and change.

What should I look for?

You should seek an organization that blends data science in its approach to mitigating bots. Pay close attention to the effectiveness of their machine learning algorithms in detecting novel or changing attacks and find out whether they use a combination of supervised and unsupervised machine learning models; supervised models are trained to quickly detect previously identified attack patterns, whilst unsupervised models are ideal for identifying suspicious activity, flagging even previously unseen attacks. Seek use cases and data demonstrating efficacy.

Robustness: "Can motivated attackers bypass the solution?"

Many bot management solutions use client-side technology like JavaScript or mobile SDKs to monitor web traffic and categorize it as human or bot. However, client-side bot management is becoming outdated.

As JavaScript code is exposed to the client, hackers and bot operators know what identifying factors the solution is looking for and can cheat the system to pass through undetected. Although some vendors obfuscate their JavaScript to combat this, motivated attackers regularly de-obfuscate code, undoing this work and forcing more effort for the vendor and target business.

What should I look for?

Before trusting that the most dangerous attackers will be slowed down by your bot management solution, research whether there are known bypass techniques for the technology it relies upon. In most cases, client-side detection technology can be reverse engineered by motivated threat actors.

This is not the case with server-side bot detection tools. As no code is exposed to the client, bot operators have no visibility of bot identification methods and cannot reverse engineer a way around such solutions.

Implementation: "Does your solution integrate easily with our existing technology stack?"

Every business has a different set of technologies working together in different ways, and adding a new tool to the mix is often challenging. Conflicts add time and effort to getting detection up and running.

Implementation should be as straightforward as possible, with clear documentation and options to integrate with technologies your business already uses, such as your CDN.

Whilst many bot management tools offer quick installation of JavaScript code or mobile SDKs, the need to continually update these 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. This is especially inefficient when deployed across multiple sites and applications.

Rather than using JavaScript and SDKs, server-side bot management solutions offer full visibility of web, mobile and API traffic in one package. These are maintained by the vendor meaning you'll always automatically have the latest protection across your entire estate.

What should I look for?

Be wary of solutions that require any hardware or client-side technology to be installed or maintained, as these are likely to be from a previous generation.

Server-side solutions have the benefit of quick implementation across not just websites, but also mobile applications and APIs with minimal setup or maintenance compared to client-based or hardware-dependent bot management solutions.

Deployment should also not take a whole team away from other tasks. Pay attention to the implementation timescales and resource requirements, both in the initial engagement and as an ongoing activity. Maintaining the tool should be the job of the vendor whilst you focus on business as usual.

Flexibility: "Will you work with our business to develop a bespoke solution?"

Many bot management solutions claim to start blocking bots almost instantly. However, all businesses and websites are different, and the way bots attack each varies greatly. This means that a one-size-fits-all approach risks missing bot traffic or creating the opportunity for dangerous false positives.

Many bot management solutions are operated by large tech giants who rely on a large user base to generalize about vulnerabilities across industries. Unfortunately, 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.

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 defense against bad bots will suffer in the long term.

Support: "Is responsive, fully-featured support included in the price?"

Comprehensive support should be available from your bot management vendor when you need it so your business can keep running unimpeded by incidents.

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. Although not always the case, some bot management solutions bundled with CDNs or other products do not offer support specific to tackling bots.

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.

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.

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.

Any quote should be customized to your needs, include everything needed to provide full protection, whilst being clear and upfront.

Expertise: "Will I have access to the latest insights and technology?"

As bot management has become a crucial component in a business's security stack, many vendors have acquired and 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 threat research is required just to keep pace.

When you buy bot management, don't just expect a tool – expertise into bot attacks that's relevant to your business should also come as part of the package.

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 is closely tied to product development and ongoing support with customers, ensuring that emerging bot attacks are mitigated, and expertise is given where needed.

Find out whether there is a dedicated research function within your bot management vendor. Ask who is involved and their qualifications, and whether they have access to restricted online criminal communities; gathering intelligence on targeted attacks and the development of specific groups is invaluable in shaping defensive strategies.

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

Bot management aims to protect your business's reputation, so you should engage with a vendor confident in their own reputation. Ultimately your chosen solution must be able to show that it will be effective and reliable in detecting and mitigating the bot threats most likely to damage your business.

What should I look for?

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 delivers.

Also, seek feedback from current or former clients of each solution you assess about all the points raised in this guide, and read reviews on portals like G2. Find out which awards and industry accolades have been won for further third-party validation and be diligent in checking which industry standards they are maintaining.

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 of both broad and targeted attacks
- [ ] Provides both clear and detailed reporting on each attack
- [ ] Is proven to have a very low false positive rate
- [ ] Can't be bypassed by attackers using known exploits
- [ ] Integrates easily with your existing technology
- [ ] Is not reliant on client-side detection or hardware integrations
- [ ] Is configured and tailored to your business rather than 'out-of-the-box'
- [ ] Has simple and straightforward pricing, which includes a full support package
- [ ] Has evidenced expertise in handling threats relevant to your business
- [ ] Includes industry-leading research on bot attacks by experts in the field
- [ ] Can evidence an excellent reputation in the industry with recognized accolades

NETACEA

Choosing the right bot management solution

Choosing the right bot management solution is a major decision for any business. This guide contains the essential requirements for a bot management solution to provide the best possible protection against bot threats. This has included not only technological considerations but also the vendor's overall approach to research, development, support and pricing.

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 organization.

This partnership, along with our innovative Intent Analytics™ technology and recognized excellence in threat research, 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 netacea.com/why-netacea or talk to our team today at hello@netacea.com.