

Top 10 Considerations for BOT MANAGEMENT





Which Bot Management Solution Is Right for You?

If you picked a website at random, what you'd find might surprise you. You would probably discover that, according to Akamai internal research, automated web robots, or bots, are responsible for between 30% and 70% of the total traffic to websites today. That simple statistic belies a complicated truth. Knowing about bot traffic is one thing. Understanding what to do about it – and then doing it – is much more challenging.

The bot management market is an evolving one, with many vendors of different sizes, experiences, and capabilities.

However, the one thing that they have in common is marketing – everybody says that they can solve your problem. You need to learn how to see through the marketing and get to the capability. To cut through the noise and get to the result. You need to know how to evaluate bot management solutions and understand what the differences mean for you.

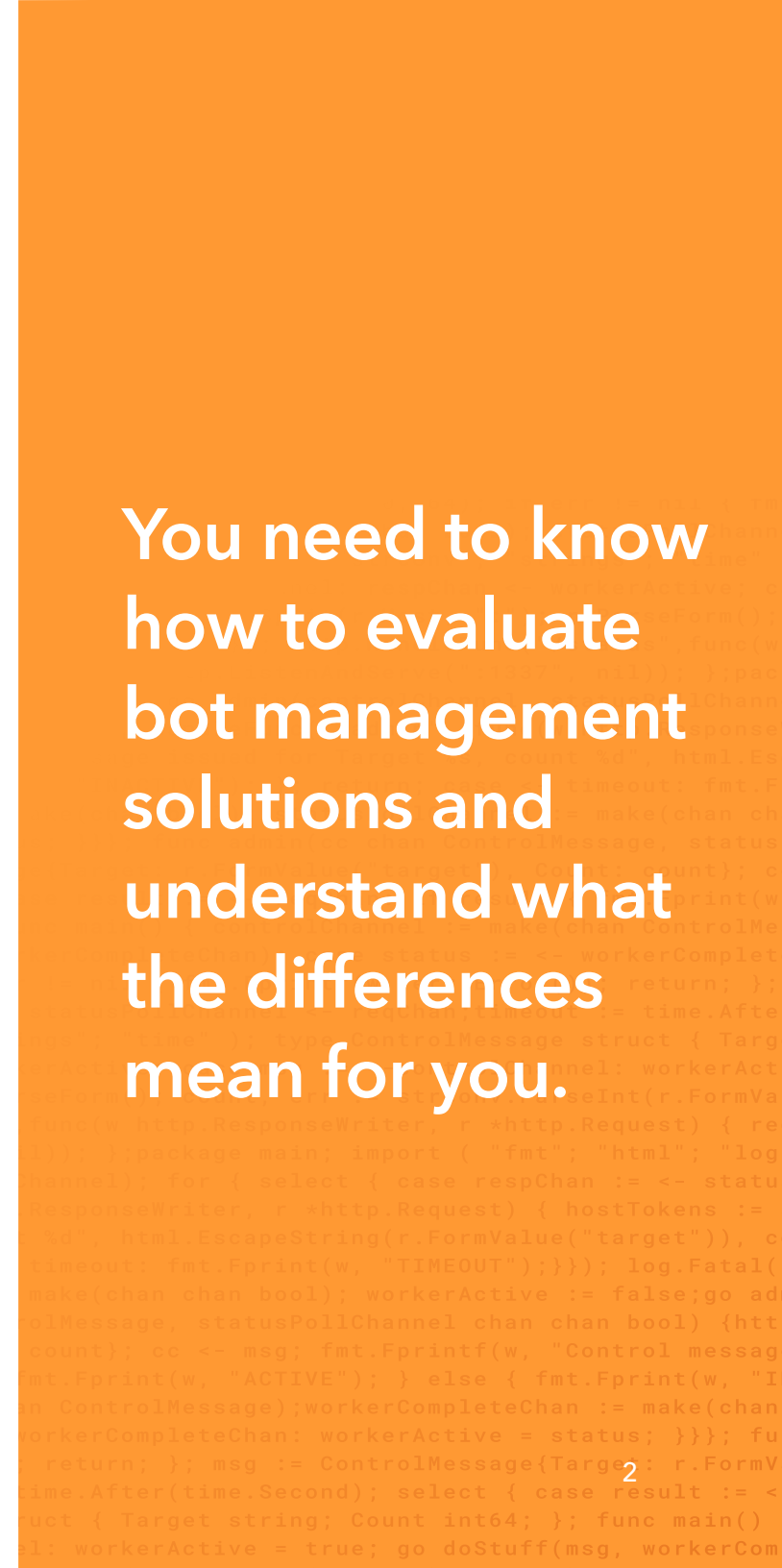
That is what this e-book is for. Read on.

Making the Right Choice

Like any tool, the right bot management solution will be the one that gets the job done. That helps you achieve your goals. That allows you to **support your business while controlling all of the bad stuff** that keeps you up at night. How do you know a solution will do that, without gambling with your budget and a year or more of your time to find out? Here's a list of the top 10 things to consider when selecting a bot management solution.

| | |
|-----------------------------|----|
| 1. Effectiveness | 3 |
| 2. Resilient Protection | 4 |
| 3. False Positives | 5 |
| 4. Flexible Actions | 6 |
| 5. Visibility and Reporting | 7 |
| 6. Protecting APIs | 8 |
| 7. On-Prem vs. Cloud | 9 |
| 8. Development Overhead | 10 |
| 9. Site vs. Page | 11 |
| 10. Managed Services | 12 |

You need to know how to evaluate bot management solutions and understand what the differences mean for you.



1. Effectiveness



Some vendors claim to detect 99.9% of all bots – that’s when you know they’re big on marketing. If you think about it for even a second, it falls apart. **How can a vendor claim to detect 99.9% of all bots without detecting with certainty 100%?** And if you knew with certainty what 100% of the bot population was, why would you only detect 99.9%?

Every solution can detect bots – the question is how many. Because bots are always changing, it’s impossible to objectively measure effectiveness. But you can measure the sophistication of the bots you are detecting. Arm yourself with an understanding of the bot landscape and knowledge of bot detection technologies, and how they compare. Make sure that whatever solution you’re looking at can detect the most sophisticated bots you’re likely to see.

Considerations:

- Understand which bot detection technologies the solution employs – and how sophisticated they are – to know what to expect at a high level.
- Not all implementations of a technology are the same. Compare similarly marketed solutions to see how well they work in your environment.
- Think like an attacker – are there attack tools available today that get around a solution’s detections? That might not be good enough.

**Make sure
that whatever
solution you’re
looking at can
detect the most
sophisticated
bots you’re
likely to see.**



2. Resilient Protection

When you block a bot, it doesn't go away. It keeps coming back, while mutating in an attempt to evade your detections. Many bot management solutions can detect the bots (at least some of them) initially, but then lose the bots after they start mutating. **Make sure the solution you select can learn and evolve over time** to consistently help solve your problems in the long term.

Considerations:

- Look for a solution with the most sophisticated bot detection technologies (like user behavior analysis). These will remain effective longer as the bots mutate.
- Ask for proof or references from other customers who have deployed the solution to see if it has remained effective over time.



Many bot management solutions can detect the bots initially, but then lose the bots after they start mutating.



3. False Positives

When a bot management solution shows it blocked a bot, *how do you know that the system actually blocked a bot and not a legitimate user?* Many vendors play fast and loose with false positives. For some, being able to show customers that they blocked lots of “bots” is more important than making sure that they’re not blocking valid traffic – humans or “good” bots that are valuable to your company. But you want to solve your bot problem without getting in the way of your business. You need to have confidence that the vendor you’re partnering with cares about accuracy and the impact of false positives.

Considerations:

- Does the vendor leave it up to you to tune for false positives or does it invest in minimizing false positives themselves?
- Does the vendor suggest using a CAPTCHA? That’s often a dead giveaway. Users hate them, but it’s easier for a vendor to offer a CAPTCHA than 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.

You want to solve your bot problem without getting in the way of your business.

4. Flexible Actions

Most bot management solutions take a security approach to the problem. They assume all bots are bad – so they should be blocked – except for individual bots you know are good (which you must explicitly add to an allow list). But what about a “good” bot that also happens to kill your website performance? Or emerging consumer services that allow your customers to connect with you in new and different ways? The fact is that bots come in all shapes and sizes, and their impact on you is rarely clear-cut. In fact, even the same “good” bot may have a different impact on your business depending on the time of day it’s operating.

You need the flexibility to apply different actions on different types of bots based on their business and IT impacts on you – especially when those impacts vary based on location, time of day, or seasonality.

Considerations:

- Does the solution allow you to create different categories for different types of bots, or is it just good and bad?
- What types of actions does the solution support? Just block and CAPTCHA? Or does it support advanced actions like slow and serve alternate content that help you better shape your traffic?
- How flexible is the solution in managing the different bots that you see? Is it another hammer, or can it surgically apply actions based on the time of day, by percentage of traffic, or by URL?

Bots come in all shapes and sizes, and their impact on you is rarely clear-cut.

5. 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. When it comes to a solution that can block your users, you don't want a black box. You need a solution that gives you the detailed reporting you need to support your business and accelerate your speed to insight.

Considerations:

- Does the solution provide reporting capabilities that allow you to zoom in on specific bots, botnets, or bot characteristics?
- Can you investigate that spike in traffic and look at individual requests? Sometimes, you need to see request details to know what to do.
- How does the reporting tie in with that of other security solutions? Can you analyze your traffic holistically, or are they separate panes of glass?


When it comes to a solution that can block your users, you don't want a black box.

6. Protecting APIs


Regardless of vendor or solution, the more sophisticated bot detection technologies available 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 SDK that can incorporate the vendor's most sophisticated bot detections into your mobile apps.
- While not always as effective as other active detections, a reputation-based approach may be a good option for protecting APIs that support third parties that may not have access to an SDK.



Without protecting your APIs, bots will simply migrate from your web pages to your APIs.



7. On-Prem vs. Cloud



It's the age-old debate – the chicken or the egg? “Star Trek” or “Star Wars”? On-premises or in the cloud? Bot management solutions come in all shapes and sizes. Some vendors have appliances. Others architect them as cloud-based solutions. You have to figure out what's right for you; but **consider how the solution will fit into the rest of your web infrastructure**. Are your web servers on-premises or in the cloud? Do you have one data center or multiple? Are you using a content delivery network (CDN)? All of these variables will affect your choice.

Considerations:

- What are your scale requirements? Understand if an appliance deployed on-premises can support any expected growth or spikes in traffic.
- Do you need to offload traffic from your origin? An on-premises appliance still requires traffic to be delivered to your data center, whereas a CDN can manage the bot traffic in the cloud.
- If you use a CDN, what are the implications of deploying another cloud-based service in front of your website?

**A solution
should protect
your apps, no
matter where
they sit.**



8. Development Overhead



Is your website or web application the lifeblood of your business? Are the requirements for uptime so stringent that you can only make changes to your application within predefined time windows? If yes, then **you need to know which application changes a proposed solution will require**. Some vendors need you to change your application to make an API call to them. Others require you to hard-code their JavaScript into any page you want to protect. That means you might now have to add the solution into your application release lifecycle. Not only that, but any time the vendor changes their solution or JavaScript code, you might have to change your application as well.

Considerations:

- How does the solution deploy? Is it an inline solution that sits in front of your application? Or does it sit out-of-band?
- If the solution site is out-of-band, what kind of application changes does it require in order to work, and do you have the resources to make those changes?

Bot management should help grow your business, not slow it down.



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 against your product pages. Content scraping against your value-added digital content. Credential abuse attacks against your login pages. 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 of 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 of your bot problems, whether they're credential abuse, web scraping, or content aggregation?



**Make sure
that the solution
can help you
address all of your
bot problems,
whether they affect
your entire site or
specific pages.**



10. Managed Services



You need to manage the bots to control their impacts 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*. 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 bot-specific resources expertise required to get the most out of a solution yourself?
- Does the bot management vendor offer professional services or does it just sell products?
- Does the vendor provide attack support that you can leverage to respond to security events at any time, even in the middle of the night?

You need someone who can connect the bots back to your core problems, and design and implement a strategy to address those problems.



Not All Bots Are the Same – Neither Are Bot Management Solutions

If your website is being overrun with bot traffic, you may be tempted in the heat of the moment to buy anything that promises to solve your bot problem.

But before you panic buy, make sure you think through the top 10 considerations for bot management so you get the best solution for your unique situation and needs.



Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or [@Akamai](https://twitter.com/Akamai) on Twitter. You can find our global contact information at akamai.com/locations. Published 07/20.