radware

How to Evaluate Bot Management Solutions

10 REASONS WHY DEDICATED BOT MANAGEMENT SOLUTIONS ARE ESSENTIAL

"Bad" bots now constitute one of the gravest threats to businesses. Malicious bot traffic can degrade website performance, tie up online inventory, compromise personal data and lead to increased customer turnover/loss of revenue. By targeting websites, mobile applications and APIs, they cause an array of business problems, such as account takeover, application DDoS, API abuse, web scraping, spam creation, skewed analytics and ad fraud.

Alternatively, good bots assist in the growth and development of the web. They crawl site pages to determine SERP rankings and keep real-time websites updated with data or help consumers find the best price for a product or discover stolen content. Being able to distinguish between good and bad bots is imperative for today's businesses. According to Radware's *Web Application Security Report*[1], 79 percent of businesses cannot accurately distinguish between good and bad bots.

The escalating intensity of global bot traffic and the increasing severity of its overall impact mean that dedicated bot management solutions are crucial to ensuring business continuity and success. This is particularly true since more sophisticated bad bots can now mimic human behavior and easily deceive conventional cybersecurity solutions/bot management systems.

Building and maintaining an in-house bot mitigation solution are resource intensive and require ongoing tuning and exception handling to avoid false positives, but are beyond the capabilities of all but the largest organizations. Leading analyst organizations such as Forrester Research and Gartner are increasingly underscoring the need for bot management solutions for organizations of all sizes.

Few resources exist to help companies evaluate bot mitigation solutions, and there is even less of a consensus as to which features and capabilities security specialists should look for when evaluating a solution. This ebook provides an overview of the key solution capabilities required to successfully manage bot traffic when evaluating these solutions.

EVALUATION CRITERIA

Addressing highly sophisticated and automated bot-based cyberthreats requires deep analysis of bots' tactics and intentions. According to Forrester Research's *The Forrester New Wave™: Bot Management, Q3 2018* report, "Attack detection, attack response and threat research are the biggest differentiators. Bot management tools differ greatly in their detection methods; many have very limited — if any — automated response capabilities. Bot management tools must determine the intent of automated traffic in real time to distinguish between good bots and bad bots."

When selecting a bot mitigation solution, companies must evaluate the following criteria to determine which best fit their unique needs.

Basic Bot Management Features

Organizations should evaluate the range of possible response actions — such as blocking, limiting, the ability to outwit competitors by serving fake data and the ability to take custom actions based on bot signatures and types. Any solution should have the flexibility to take different mitigation approaches on various sections and subdomains of a website, and the ability to integrate with only a certain subset of from pages of that website — for example, a "monitor mode" with no impact on web traffic to provide users with insight into the solution's capabilities during the trial before activating real-time active blocking mode. Additionally, any enterprise-grade solution should be able to be integrated with popular analytics dashboards such as Adobe or Google Analytics to provide reports on nonhuman traffic.

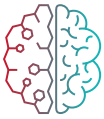
[1]https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=8307fab3-5339-4cb4-afbd-80358438c908

Capability to Detect Large-Scale Distributed Humanlike Bots

When selecting a bot mitigation solution, businesses should try to understand the underlying technique used to identify and manage sophisticated attacks such as large-scale distributed botnet attacks and "low and slow" attacks, which attempt to evade security countermeasures.

Traditional defenses fall short of necessary detection features to counter such attacks. Dynamic IP attacks render IP-based mitigation useless. A rate-limiting system without any behavioral learning means dropping real customers when attacks happen. Some WAFs and rate-limiting systems that are often bundled or sold along with content delivery networks (CDNs) are incapable of detecting sophisticated bots that mimic human behavior.

The rise of highly sophisticated humanlike bots in recent years requires more advanced techniques in detection and response. Selection and evaluation criteria should focus on the various methodologies that any vendor's solution uses to detect bots, e.g., device and browser fingerprinting, intent and behavioral analyses, collective bot intelligence and threat research, as well as other foundational techniques.



A Bot Detection Engine That Continuously Adapts to Beat Scammers and Outsmart Competitors

- How advanced is the solution's bot detection technology?
- Does it use unique device and browser fingerprinting?
- Does it leverage intent analysis (machine learning detection models that ascertain each visitor's intent and provide significantly higher accuracy compared to simple interaction-based behavioral analysis) in addition to user behavioral analysis, collective bot intelligence (i.e., "wisdom of the crowd"), dynamic Turing tests, etc.?
- How deep and effective are the fingerprinting and user behavioral modeling?
- Do they leverage collective threat intelligence?

Any bot management system should accomplish all of this in addition to collecting hundreds of parameters from users' browsers and devices to uniquely identify them and analyze the behavior. It should also match the deception capabilities of sophisticated bots. Ask for examples of sophisticated attacks that the solution was able to detect and block.

Impact on User Experience — Latency, Accuracy and Scalability

Website and application latency creates a poor user experience. Any bot mitigation solution shouldn't add to that latency, but rather should identify issues that help resolve it.

Accuracy of bot detection is critical. Any solution must not only distinguish good bots from malicious ones but also most enhance the user experience and allow authorized bots from search engines and partners. Maintaining a consistent user experience on sites such as B2C e-commerce portals can be difficult during peak hours. The solution should be scalable to handle spikes in traffic.

Keeping false positives to a minimal level to ensure that user experience is not impacted is equally important. Real users should never have to solve a CAPTCHA or prove that they're not a bot. An enterprise-grade bot detection engine should have deep-learning and self-optimizing capabilities to identify and block constantly evolving bots that alter their characteristics to evade detection by basic security systems.

Distinguish Between "Good" and "Bad" APIs

As the use of API increases (IoT, microservices, integration, machine-to-machine communication, etc.), bot mitigation for APIs must take precedence to protect sensitive data from failing into the wrong hands. Detecting malicious behavior on APIs is different than web and mobile applications and requires distinguishing between "good" and "bad" API calls.

- Does the solution use a dedicated protection model to safeguard API data transactions or does it use a generic approach that is typically leveraged for websites?
- How does your API server uniquely identify (fingerprint) a client device to validate the authenticity of requests being made to the server?
- Can the solution identify authentic access patterns to pinpoint malicious access attempts?
- Does the bot mitigation engine perform a detailed intent analysis to confirm the API request isn't trying to take over user accounts, scrape data or cause denial-of-service?

Extensibility and Flexibility

True bot management goes beyond just the website. An enterprise-grade solution should protect all online assets, including your website, mobile apps and APIs. Protecting APIs and mobile apps is equally crucial, as is interoperability with systems belonging to your business partners and vital third-party APIs.

Flexible Deployment Options

Bot mitigation solutions should be easy to deploy and operate with the existing infrastructure, such as CDNs and WAFs, as well as various technology stacks and application servers. Look for solutions that have a range of integration options, including web servers/CDNs/CMS plugins, SDKs for Java, PHP, .NET, Python, ColdFusion, Node.js, etc., as well as via JavaScript tags and virtual appliances.

A solution with nonintrusive API-based integration capability is key to ensuring minimal impact on your web assets.

Finally, any solution provider should ideally have multiple globally distributed points of presence to maximize system availability, minimize latency and overcome any internet congestion issues.

Is It a Fully Managed and Self-Reliant Service?

Webpage requests can number in the millions per minute for popular websites, and data processing for bot detection needs to be accomplished in real time. This makes manual intervention impossible — even adding suspected IP address ranges is useless in countering bots that cycle through vast numbers of addresses to evade detection. As a result, a key question that needs to be answered is does the solution require a specialized team to manage it, or does it operate autonomously after initial setup?

Bot mitigation engines equipped with advanced technologies, such as machine learning, help with automating their management capabilities to significantly reduce the time and workforce needed to manage bots. Automated responses to threats and a system that does not require manual intervention considerably reduce the total cost of ownership.

Building vs. Buying a Specialized Solution

Large organizations have resources to develop their own in-house bot management solutions, but most companies do not have the time, resources or money to accomplish that. Building an adaptive and sophisticated bot mitigation solution, which can counter constantly evolving bots, can take years of specialized development.

Financially, it makes business sense to minimize capex and purchase cloud-based bot mitigation solutions on a subscription basis. This can help companies realize the value of bot management without making a large upfront investment.

Data Security, Privacy and Compliance Factors

A solution should ensure that traffic does not leave a network — or, in case it does, data should be in an encrypted and hashed format to maximize privacy and compliance. Ensuring that the bot mitigation solution is compliant with the GDPR regulations pertaining to data at rest and data in transit will help avoid personal data breaches and the risk of financial and legal penalties.

CONCLUSION

For organizations both large and small, securing the digital experience necessitates the need for a dedicated bot management solution. Regardless of the size of your organization, the escalating intensity of global bot traffic and the increasing severity of its overall impact mean that bot management solutions are crucial to ensuring business continuity and success. The rise in malicious bot traffic, and more specifically, bots that mimic humanlike behavior and require advanced machine learning to mitigate, require the ability to distinguish the wolf in sheep's clothing.

LEARN MORE ABOUT **BOT MANAGER** OR **CONTACT RADWARE** WITH ANY QUESTIONS.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.