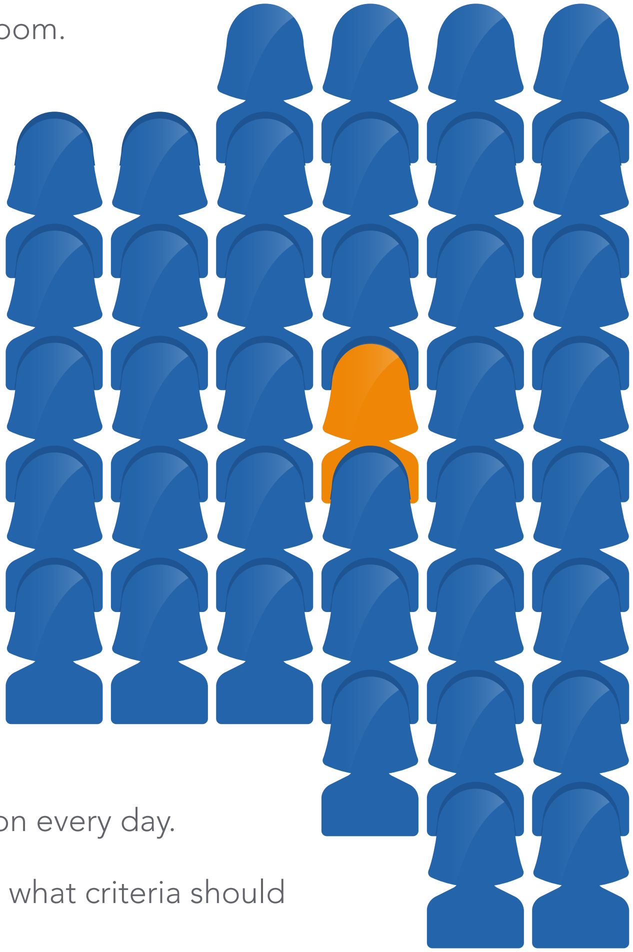
CEQUENCE®
SECURITY

Top 7 Selection Criteria for Automated Bot Prevention Solutions

How to ensure long-term protection against today’s evolving automated attacks

EBOOK

It’s Getting Crowded in Here



Today, bots are becoming more than just a security threat. Their contributions to very real lost revenue and customer dissatisfaction are now getting noticed in the boardroom. Many businesses are coming around to realizing that they are evolving into a serious business problem.

As a result, the automated bot prevention market is now packed with both old and new vendors, each trying to solve the fast-escalating challenge for enterprises across the globe. However, not everyone’s approach is equally effective.

Today’s commercially available botting platforms can defeat most first-generation bot prevention solutions just by using their built-in evasion capabilities. As a result, enterprises that implemented early bot prevention solutions see reduced efficacy today as their incumbent tools fail to address the evolving bots. This has pushed these organizations back into the market to seek better alternatives in hopes of finding a solution that will be effective.

This trend is confirmed by increased outreach to vendors like Cequence Security and industry analysts, who see rising client inquiries about bot prevention every day.

So, with multiple options and a rapidly escalating number of automated attacks, what criteria should enterprises evaluate when selecting their next bot prevention solution?

#1: Fast Deployment and Time to Value

Key Criteria

Look for a bot prevention solution that you can deploy across the entire attack surface (web, mobile, and API) in less than one hour, and that provides effective bot mitigation in less than one day.

Why?

When faced with today's sophisticated bot attacks, enterprises lose revenue, brand value, customer experience, and customer loyalty while also incurring fraud losses.

Rapidly stopping these should be a top priority for security and business teams. Therefore, select a bot prevention solution that you can deploy quickly across all applications and APIs. Don't stop at just the ones currently being targeted either. Ensure that coverage extends across all your applications and APIs that attackers may turn their attention to in the future. In addition to deploying quickly, be sure to check how long it will take to realize policy-based mitigation, which will instantly begin to deliver value as bots are detected and stopped — even if an attacker retools.

Pitfalls to Avoid

- **Solutions that require application integration and new code deployment** require extensive testing and validation and may still break applications transparently. Depending on the complexity of the integration, especially for mobile applications/endpoints, this can take months and leaves you vulnerable to bot attacks in the meantime.
- Any solution that **forces security teams to depend on application teams for protection** creates organizational challenges and can lead to finger-pointing among peers.
- **Solutions that require a forced upgrade of mobile applications** across the user population cause tremendous friction among users. It also delays the solution's effectiveness until a majority of users have upgraded to a common minimum version.

#2: Don’t Forget API Protection

Key Criteria

Look for a bot prevention solution that can protect pure APIs with the same high efficacy as web and mobile applications.

Why?

As the adoption of cloud and microservices-based architectures increases, explosive growth in APIs at enterprises has followed. Large monolith applications are often now broken down into microservices that provide the same business logic through APIs. These same APIs are a prime target of bots because they are:

- Easy to attack as they are stateless and often less complex than a web form.
- Well documented for developers and partners, making writing bots to target the API easier.
- Usually poorly protected or not protected at all.

Pitfalls to Avoid

- Avoid solutions that require application integration. These solutions are not built around APIs. They rely on telemetry from end-user devices for their detection, and, in the case of APIs, telemetry may not be available.
- API security solutions, like 42 Crunch, don’t solve complex bot problems. Using a purpose-built API security solution to fight bots means taking bot traffic too deep in your infrastructure.

#3: Ensure Broad Use Case Coverage

Key Criteria

Make sure the solution can solve your specific bot problem(s).

Why?

As documented by the OWASP Automated Threats to Web Applications, bots come in many flavors. Bots-as-a-service platforms will often combine multiple threats from the list, increasing the sophistication of the attack and making it difficult for first-generation bot prevention offerings to stop it. Your next bot prevention tool needs to handle all 20+ of the automated threats listed equally well and simultaneously.

Pitfalls to Avoid

- Bot prevention solutions that were built around addressing Account Take Over (ATO) attacks can struggle to deal with other threats, such as scraping and automated shopping.

  Example: Financial services and insurance companies may have selected an ATO prevention-focused solution that is unable to stop competitive scraping attacks.

- Retailers dealing with "hype sales" should ensure their solution of choice can effectively prevent automated shopping bots that combine scraping, ATO, fake accounts, and enumeration attacks.

#4: Retooling Resiliency

Key Criteria

Your bot prevention solution needs to demonstrate sustained efficacy against bots retooling.

Why?

We often engage with customers who implemented bot prevention quickly while under severe pressure from automated attacks and found the solution immediately had a positive impact. Unfortunately, over time, the bots evolved to a point where the selected tool could no longer effectively detect or mitigate the bots, who had changed tactics.

The source of the decreased efficacy can be found in numerous online forums and GitHub repos. Bot managers continually collaborate and retool to evade detection, often-times by reverse-engineering the JavaScript or SDK used to collect telemetry. When selecting a bot prevention solution, choose one that requires no JavaScript or SDK integration and perform reference checks to confirm that the solution provides sustained efficacy against bots retooling.

Pitfalls to Avoid

- Solutions that **require the use of a visible (reversible) agent (e.g., JavaScript or SDK)** to collect telemetry are easy for attackers to retool against and evade.
- Look for solutions that **do not have videos, tutorials, or GitHub repos** that document how to defeat the solution.

#5: Avoid User Friction

Key Criteria

Avoid solutions that add user-challenge-based systems like CAPTCHA and virtual waiting rooms.

Why?

Improving security at the expense of user experience is never a good idea. CAPTCHA-based solutions, where real users solve visual challenges to use an online service, cause friction; they are not a bot prevention solution per se. When used in conjunction with bot prevention, CAPTCHAs are trying to overcome a solution deficiency at the expense of user experience. It's even worse if for VPN or anonymous browser users, who will see CAPTCHAs constantly.

Additionally, virtual waiting rooms are merely a mechanism that enables CDN-based bot offerings to (try) to keep up with the volume of bot transactions they are processing. They cause significant user frustration but, in the end, have little to no impact on bot prevention.

Pitfalls to Avoid

- CAPTCHAs that are fun? There is no such thing. Bots can defeat CAPTCHAs by using Optical Character Recognition (OCR) or mechanical turks to solve 1000 CAPTCHAs (including the fun ones) for just $3.99.
- E-mail reputation-based CAPTCHAs — Botters easily get around them by using services that harvest new e-mail addresses and increase their reputation by sending e-mails on those accounts.
- Solutions that rely on virtual waiting rooms as a bot prevention feature or benefit — bots quickly bypass these leaving legitimate customers waiting (and potentially shopping your competition).

#6: No Black Boxes

Key Criteria

Ensure your bot prevention solution provides you, the user, with access to detailed information about detection, mitigation, and the ability to modify policies as needed.

Why?

No security solution is perfect. While a good bot prevention solution will do a great job at stopping bots, occasionally, it will have false positives. Every security solution does. In such cases, the ability to respond rapidly is time sensitive. Does your existing solution require professional services to provide visibility into each transaction blocked?

Ideally, your bot prevention solution should provide fingertip access to this data so you can perform timely root cause analysis. The ability to export the data to a reporting or SEIM tool to analyze the business impact of high-volume bot attacks is equally critical.

Pitfalls to Avoid

› **Avoid solutions that claim 100% efficacy** without giving you access to the management dashboard for visibility.

› **"White glove" professional services** to support black box solutions limit your access.

#7: Plays Well With Others

Key Criteria

Select a bot prevention solution that integrates with your security ecosystem to help you improve your overall security posture.

Why?

Combining telemetry and detection metadata from your bot prevention solution with other security solutions has a multiplying effect. For example, joining bot detection telemetry with anti-fraud solution data can help accelerate fraud resolution. Conversely, security intelligence from anti-fraud teams and solutions can also improve bot prevention efficacy.

Automating the data collection and analysis also will help eliminate the manual, time-consuming review and validation of new (and sometimes fake) account creation. The ideal bot prevention solution should integrate via APIs with your security ecosystem of fraud, SIEM, SOAR, and other tools to improve the overall security and risk posture of your organization.

Pitfalls to Avoid

› Rethink black box solutions with great-looking UI, but no reporting, data import/export, or API integrations.

› "White glove" professional services required to support data analysis or transfer requests will dramatically reduce your flexibility.

Conclusion

While you may feel pressured to select a solution quickly due to ongoing challenges from bot attacks, be sure the tool you choose will extend sustained protection to your applications and APIs. Keep the criteria above in mind, and you'll find yourself with a solution that will work for your future security needs long term, even after attackers retool and evolve in sophistication.

As more of our personal and professional activities move to digital experiences, the ability to strongly protect those interactions and applications from malicious bots has become imperative. A bot prevention solution that adapts to the changing threat landscape, as well as your changing application environment, enables your organization to thrive and grow while protected, making it a valuable component of your business strategy and success.

CEQUENCE®
SECURITY

100 S. Murphy Avenue, Suite 300, Sunnyvale, CA 94086, 1-650-437-6338, info@cequence.ai, www.cequence.ai