DATADOME

GUIDE

2023

Bot Management & Online Fraud Prevention Buyer's Guide

datadome.co

Table of Contents

Assessing Your Need for Bot & Online Fraud Protection

As a cybersecurity leader, you've likely experienced damaging online fraud attacks—whether in the form of credential stuffing, card cracking, account takeover (ATO), chargeback fraud, or scalping. You are probably aware that fraudsters require automation (bots) to scale and distribute their attacks against businesses like yours.

You might be considering bot protection for one or more reasons:

- Your business leadership is asking you for a fraud prevention plan.
- Key business or operational metrics—ranging from conversion rates and payment decline rates to server overloads and bounce rates—are flashing red.
- You are grappling with the challenge of protecting your business and customers against fraudsters without degrading your user experience.
- Your operations teams are overwhelmed with blocking bots manually.
- You are being asked to move quickly while saving resources on a tight budget.

You may even have a bot management tool in place, but continue to experience painful recurring symptoms of malicious, fraudulent traffic. If any of this sounds familiar, this is the right guide for you.

Why is bot protection critical to online fraud prevention?

If your website, mobile application, and/or API processes payment information, or any other sensitive data, fraudsters are going to target and attack your platform—no matter what. And **fraudsters require bots** to scale and distribute their attacks against online enterprises.

That's why **bot protection is the foundation of online fraud prevention.**

Bot attacks are not the exception, but the rule for most online and e-commerce businesses because bots make it easy and cheap for bad actors to overwhelm and bypass basic security measures. In fact, cybercriminals use more sophisticated tools and techniques every day, constantly adapting to circumvent cybersecurity software.

Their goal? To monetize *any exposed digital surface or data* that can be stolen from your business and your customers.

Online fraudsters aim to steal your **website content** and **products**, as well as your customers' personal information, **accounts**, and **payment details**. Effective mitigation depends on the specific issues bots are causing for your business.

Ask yourself these questions:

- What are the particular needs of my organization?
- What are the pain points and challenges we are looking to resolve?

Are scrapers stealing your competitive advantage by taking your content or pricing and reposting it elsewhere? Are they ruining your site's speed and performance? Are scalpers alienating your customer base by snagging your limited-edition products before real customers can purchase them?

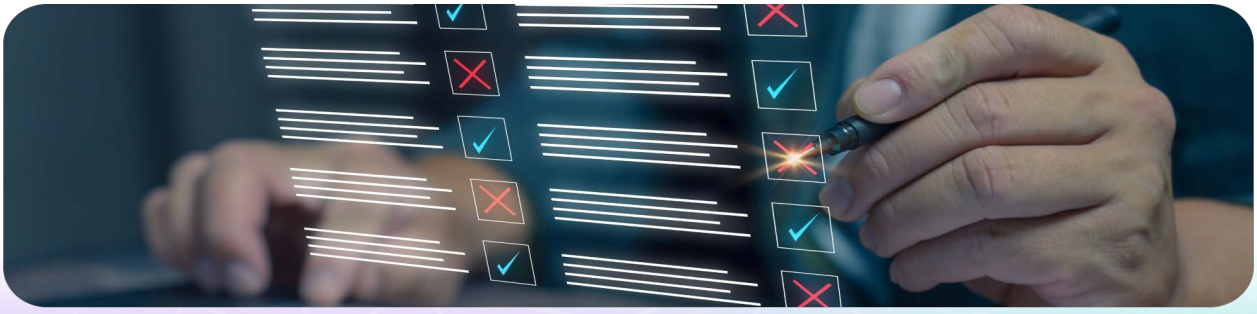
At minimum, the bot management solution you choose must address your organization's primary pain points. If you're in the midst of a bot attack, you need to stop the immediate pain as fast as possible. But any bot mitigation you deploy today could become your long-term solution, so it is important to choose carefully.

Today's sophisticated bot attacks can only be stopped by specialized and advanced bot protection—built to **accurately** detect bots and online fraud, and to keep malicious traffic away from your websites, applications, and APIs.

Choosing the Right Solution

Realizing your business needs bot protection to reduce your online fraud risk is a vital first step, but there are many bot management tools to choose from. **With so many options on the market, how do you determine which bot management solution will best meet your specific needs?**

This buyer's guide will help you make a thoughtful, informed decision by outlining the key capabilities to consider when evaluating different bot management platforms. We will help you review your business' specific needs and determine which bot and online fraud protection on the market will be your best fit.



How are bots attacking your organization?

Scraping

Scraping is the collection of data from your website, app, and/or API, most often for malicious purposes, such as undercutting your prices or reselling/reposting your content for the fraudster's financial gain. Scraping is often performed by many bots using distributed proxies.

Scraping is the **most common type of bot attack**, and is increasingly used as a "gateway threat" to other, more damaging attacks, such as scalping. In fact, our customer data shows that scraping and scalping combined account for *98% of bot attacks*.

Common tools used for scraping prevention include:

- **Traditional CAPTCHAs:** Only about 50% effective today, traditional CAPTCHAs are easily bypassed by fraudsters using CAPTCHA farms and CAPTCHA solve bots.
- **Web Application Firewalls (WAFs):** WAFs can block *known threats* but cannot detect new threats, making it a manual process to add new rules after attacks happen.

Both traditional CAPTCHAs and WAFs fall short of stopping today's advanced scraping attacks, which use bad bots to request access to your websites, applications, and APIs from distributed, often residential IPs.

Scalping

Scalping involves purchasing limited-availability goods to resell at a higher cost. Scalpers use bots that can complete the checkout process far quicker than any human to snatch up and hoard as much inventory as possible. Online scalping is almost entirely automated.

Anti-bot techniques like device/browser fingerprinting, IP reputation, and behavioral analysis can help determine if a user is human or bot, so bots can be blocked without interrupting the human user experience.

The most effective bot detection techniques are expensive to execute manually, draining both money and time from enterprise teams who try to manage detection in-house. An efficient solution must evolve with the threat landscape and use the most up-to-date anti-bot techniques possible.

Account Takeover (ATO) & Credential Stuffing

ATO occurs when malicious actors use bots to gain control of user accounts, generally to perpetuate fraud, such as stored value theft, identity theft, credit card information theft, and fraudulent transactions. To execute ATO, bots conduct **credential stuffing** to test countless username-password combinations to gain access to your real users' accounts and data.

Too often, **ATO attacks go unnoticed** until bots rack up a large number of failed login attempts across several accounts. Enterprises often discover ATO too late, when the damage has escalated. In fact, **IBM reports** that stolen or compromised credentials are the most common cause of data breaches and take the longest to identify—averaging **327 days** to be discovered by businesses and costing $150,000 more on average than other data breaches.

ATO can be somewhat mitigated by multi-factor authentication (MFA)—but not stopped entirely, because attackers can outmaneuver MFA using a wide range of techniques, including man-in-the-middle, hijacked authentication APIs, SIM swaps, and social engineering.

Fake Account Creation

Fake account creation happens when fraudsters use bots to create fake user accounts on your website or application for malicious activity, such as spreading malware, influencing product reviews, or distributing false information.

Card Fraud (aka Carding or Card Cracking)

Card fraud, carding, and card cracking encompass anything related to the fraudulent use of payment card data. Both carding and card cracking use bots to test and guess missing values for stolen card data to make fraudulent purchases or transfer/steal funds.

Card fraud attacks can be detected by monitoring high volumes of small orders, orders with high shipping costs, IP address geolocation, data input and transaction speed, the address verification system (AVS), and card verification value (CVV). Trying to monitor all relevant details manually is very time-consuming, so it's best if you can automate it.

Layer 7 DDoS

Layer 7 DDoS (distributed denial of service) attacks target the application layer in the OSI model, typically in a "low and slow" manner (using extremely slow HTTP or TCP traffic that appears to be legitimate). DDoS attacks are perpetrated by huge botnets that can overwhelm most web infrastructures.

Today's easy access to bots as a service (BaaS) and machine learning (ML) tools makes DDoS more common and allow DDoS attacks to last longer than previous attacks.

DDoS attacks can be manually mitigated by increasing network capacity (which quickly becomes costly), creating new WAF rules, manual IP filters, and ad-hoc network analysis. However, each manual option is too slow and IP-based filtering (including WAFs) is ineffective against the thousands of proxy IP addresses used by bots.

Vulnerability Scanning

Fraudsters leverage malicious **vulnerability scanning** to find potential vulnerabilities across your mobile apps, websites, and APIs they can target and exploit for online fraud. Vulnerability scanning can be performed manually by humans, but is typically automated and completely performed by software programs or bots.

Most Common Concerns for Online Enterprises

A **Forrester Consulting survey** commissioned by DataDome of 100+ online commerce enterprise decision makers found that:

- **91%** feel that protection against card fraud, including card cracking, is critical.
- **90%** are concerned with protection against inventory fraud, such as scalping.
- **89%** prioritize protection against account fraud, which includes credential stuffing and ATO.
- **86%** are prioritizing user performance and app availability.
- **67%**, roughly two out of three, are focusing on mobile app and API protection.

Financial Impact of Bot Attacks

As you expand and modernize your digital presence, your attack surface also increases. Fraudsters will target your most vulnerable endpoints across your websites, applications, and APIs with increasingly sophisticated attacks.

Bot and online fraud attacks have significant impacts on bottom-line business costs, as well as customer satisfaction, brand reputation, and other key factors for e-commerce enterprises.

- **Internal Costs**
  The top internal impact on organizations of bot and online fraud attacks is the cost of **employee hours spent manually mitigating attacks**, according to a Forrester Consulting study commissioned by DataDome. Spending hours on manual bot mitigation often causes employee burnout and frustration, as well as stealing your team's focus away from revenue-driving activities.

- **External Costs**
  In terms of the external impacts of bot attacks, e-commerce leaders report being most concerned about the **loss of customer trust**, **declining customer satisfaction**, and **reputational damages**.

But wasted time and customer churn are just the tip of the iceberg when it comes to bad bot and online fraud costs. There are more financial damages to consider:

Revenue Loss

While it is possible for the financial impact of a bot attack to be sudden, sharp, and obvious, bad bot traffic often hurts your revenue in more subtle, insidious ways:

1. **Website Downtime:** Layer 7 (application layer) DDoS attacks are typically low and slow, but can still take down your site.

   To calculate your downtime loss, divide your total annual online revenue by the number of minutes in a year (525,600) and multiply that by the number of downtime minutes you experience.

2. **Poor Site Performance:** In e-commerce, milliseconds matter. Bot traffic doesn't have to bring your site down completely to frustrate customers, it just has to *slow* it down.

   A one-second delay in page response can result in a 7% reduction in conversions. If you generate $100,000 per day, that could mean **$2.5 million** in lost sales per year.

3. **Inventory Hoarding:** Unlike scalper bots, inventory hoarding bots never complete a purchase. They simply add merchandise to the cart and refuse to check out, depleting your inventory with "pending" purchases. Then, actual shoppers get an "Out of Stock" message.

   Inventory hoarding can ruin flash sales, holiday sales, and limited-edition merchandise drops, driving away your real customers and rendering all the resources you put into your sales events a waste.

4. **Price Undercutting:** Bots can scrape and automatically undercut your prices. Price scraping steals your competitive advantage and nullifies your pricing strategy efforts, pulling your customers away as they chase lower prices.

5. **Real Cost of Reputational Damages:** Every year, multiple high-profile data breaches become front-page news, and the breaches are *costly*. In 2017, an **Equifax data breach** cost the credit bureau **$1.4 billion**. Just two years earlier, **Ashley Madison lost 80%** of its traffic due to a data breach.

Operational Expenses

1. **Abused Customer Loyalty Rewards:** Loyalty and reward programs are particularly vulnerable to attacks. Industry experts estimate (conservatively) that losses from **loyalty and reward point fraud** are around **$1 billion** every year.

2. **Increased Authentication Costs:** If any of your online services require extra authentication, it may be associated with extra fees. For example, with two-factor authentication (2FA), you may pay for an SMS text to be sent any time a user logs in.

   If your login page is hit with a **massive volume** of malicious bot requests, it can generate an SMS bill of **tens or hundreds of thousands** of dollars fast.

3. **Inflated CDN Bill:** Nearly all major content delivery networks (CDNs) have a pricing model that charges per GB used. Bot traffic increases your outbound

data transfer volume, and thereby your CDN bill, by **up to 70%** for some businesses.

4. **Higher API Bill:** Some third-party service providers use metered billing to charge for the number of API calls you make, in which case **you also pay** for every API call that is generated by a bot.

   A human visitor using a store locator might generate a handful of calls to a mapping API, while a bot trying to scrape every address in the directory could generate hundreds or thousands.

5. **Wasted Advertising Spend:** Ad fraud, click fraud, and influencer fraud are examples in which bots mimic human behavior to skew important metrics and steal millions of dollars from advertisers.

   The global **digital ad fraud loss** has climbed from $35 billion in 2018 to an estimated **$100 billion in 2023**.

Regulatory Penalties

1. **Data Privacy Penalties:** Legislators in many countries and states have introduced regulations to protect consumer privacy and data security. The best known are the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA).

   Regardless of where your business is located—if you collect data from EU or California residents, bot-driven breaches, such as unmitigated ATO attacks, will expose you to hefty penalties. For example, a famous US-based e-commerce enterprise announced in July 2021 that it had been fined more than **$875 million** (€793 million) due to alleged GDPR violations.

2. **PCI DSS Compliance Penalties:** The Payment Card Industry Data Security Standard (PCI DSS) is a standard for businesses that handle card payments.

   The 12 PCI DSS requirements include an obligation to protect cardholder data and to "address new threats and vulnerabilities on an ongoing basis." Generally speaking, **fines for non-compliance** may range from **$5,000 to $100,000 per month**.

3. **Governmental Scrutiny:** Bot traffic can bring unwanted attention to your business—both socially and legally—that will impact your bottom line.

For example, the Taylor Swift **ticketing fiasco** (directly linked to automated bots, despite planned countermeasures) put Ticketmaster under the microscope of the US Congress.

As a result, the **Justice Department reportedly** opened an **antitrust investigation** against Ticketmaster. Repercussions might include requiring the enterprise to lower its service fees, which often total 20% of face value and mostly go to the venue, with smaller shares reserved for credit card fees and Ticketmaster itself.

Congress could also decide to restrict the resale of tickets for profit, insist buyer's names be printed on every ticket, or even break up Live Nation—all of which would have major implications for the ticketing industry.

The negative financial impacts of malicious bot traffic and online fraud attacks can range from immediate to delayed and be both severe and long-lasting. That's why most enterprise leaders will tell you that finding the right bot protection will save you money in the long run, from averted costly attacks to employee hours saved from manual bot mitigation.

Future-Proofing Your Security for an Evolving Threat Landscape

As the need for bot and online fraud protection continues increasing over time, enterprise solutions must be built to proactively evolve with the rapidly-shifting threat landscape. Cybersecurity leaders must ensure the bot protection chosen today is not outpaced tomorrow by attackers or their technology. Below are some key qualifications for efficient protection.

Powered by AI & ML

Today's advanced bots leverage technology that drives **ChatGPT** and deep fakes. Modern bot management solutions **must** also incorporate artificial intelligence (AI) and **machine learning (ML)** to optimize their accuracy in recognizing new threats while maximizing efficiency and scalability.

Integration With Other Solutions

Modern security stacks leverage numerous toolsets, and bot protection is a critical component. The last thing you need is a siloed software that further complicates an already diverse array of security and CDN/cloud deployments.

Therefore, your bot management solution needs to integrate easily with your other tools and systems. A solution with **diverse integration capabilities** will help you prevent blind spots, avoid silos, and consolidate your team's alerts and notifications.

Regulatory Compliance

Depending on your industry and geographic location, you might have specific regulations and compliance mandates (such as **data privacy** and sovereignty laws) your bot and online fraud protection must meet. Unfortunately, some **government agencies have ruled** that bot mitigation tools like reCAPTCHA, for example, use data for purposes other than security, and are not automatically compliant with GDPR.

Make sure the solution you choose is designed to meet the relevant requirements, with the flexibility to respond to future compliance changes and challenges.

Ease of Deployment & Maintenance

A bot management solution must be easy to deploy and maintain in order to minimize operational disruption and maximize return on investment. Consider any potential vendor's performance and track record in ongoing support and maintenance. You should validate the quality of the customer support by checking **ratings and reviews** from peer organizations.

Flexibility & Customization

Organizations have different needs when it comes to bot management, often resulting from different threats, fraud use cases, and customer experience KPIs, among other factors. As a result, cybersecurity leaders must evaluate whether a solution offers the necessary levels of customization, flexibility, and support to meet organizational requirements, from **onboarding** to troubleshooting.

Proven Pace of Innovation

The bot and online fraud landscape is changing every day. Security vendors must stay on top of the latest techniques and tools used by cybercriminals at all times.

The only way to ensure your solution stays ahead of fraudsters is by choosing a provider with a recognized team of threat research experts to analyze and update detection models 24/7.

Another important factor is the bot management vendors' track record of product innovation and performance. Do they **anticipate bot evolution** and adapt by adding new features regularly, or is the tool still the same as it was a decade ago? Reviewing past performance can give you an idea of a vendor's sophistication and ability to deliver value over time.

Checklist: Bot Management Key Selection Criteria

Below are some key considerations to prioritize when narrowing down your bot management solution shortlist:

Purpose

- [ ] **Best of suite vs. best of breed.** 🏆

Some vendors choose to offer a variety of different services, from CDNs to SASE (secure access server edge) and WAFs (web application firewalls), in addition to a bot management tool. Unfortunately, the lack of dedicated "bot" focus usually means tools are less effective than standalone, specialized solutions against sophisticated bots.

Some vendors provide a WAF, a basic gen 1 bot management tool with only static, rules-based blocking capabilities. **WAFs are no match against today's highly sophisticated bots**, which are only detectable by equally sophisticated solutions using dynamic behavioral analysis on each request.

When it comes to bot management, a basic tool that may seem "good enough" now will ultimately fall short in stopping the most damaging bot attacks. Only a solution that proactively adapts to new threats on an ongoing basis will be effective. Look for a vendor that offers complete, **advanced bot protection** as the main solution, not as a second-class service or add-on.

- [ ] **Breadth of solutions, use cases, and supported endpoints.** 📲

Does the vendor only support websites, or do they also **protect mobile applications** and APIs? Your business must be fully protected in a consistent manner to circumvent malicious bots and online fraud.

Is it easy to extend the solution to add new use cases and endpoints to protect? Does the protection leverage both server-side and **client-side detection signals**—both of which are necessary for securing all endpoints and detecting advanced bots?

Does the vendor offer lightweight SDKs with proof of fast, successful deployment on various devices (iPhone, Android, etc.) and no added latency or impact on the mobile user experience? Will the vendor work to ensure the solution covers each endpoint equally for every use case?

Look for a solution that works on every endpoint, easily scales with your traffic, and can be used to support new use cases when needed.

- [ ] **Ease of implementation and use.** 🚀

A bot management solution should save you time and resources by protecting you on **autopilot**. It should run automatically in the background, no matter the volume of bots attempting to attack your infrastructure.

Does the software require a lot of customization to fit into your organization's architecture? Are manual interventions necessary? Does it require continuous tuning from your SecOps team to keep the protection working? How easy to understand and use is the interface?

Look for a solution that can be **integrated into your tech stack** quickly and easily to ensure quick time to value. Also, choose a vendor that provides intuitive and **easy-to-use dashboards** and reporting to keep track of the protection's performance.

Performance & Track Record

- [ ] **Accuracy & quality of bot detection & protection.** 🎯

There's no sense in deploying a bot solution that can't demonstrate detection accuracy. How accurate is the bot solution in terms of its false positive rate?

Does the vendor continuously improve its detection capabilities through threat research and collective intelligence of real-time attacks, or are there delays and gaps that lead to detection degradation over time? What kind of feedback loop is used to train and optimize the solution's **ML detection** models? Does the solution make continuous updates in real-time—and offer full transparency so you can assess its effectiveness?

Look for a vendor that transparently reports its solution accuracy in real time and delivers a low false positive rate—without sacrificing bot detection quality. Make sure that the vendor's accuracy claims don't come at the expense of **speed**, data privacy compliance, or your customers' online experience.

☐ **Performance—delivering protection without compromise.** ✅

Accuracy is key in bot detection, and so is performance. Interrogating every request every time could cripple many solutions, which is why sampling requests or using token-based techniques are common workarounds. Ask your vendor about the **number of points of presence** (PoPs) they have in your operating regions and worldwide.

Find out the solution's latency benchmarks for like-for-like detection scenarios. A legacy solution architecture or limited supported PoPs can force you to sacrifice accuracy in order to maintain a smooth user experience for online transactions. Look for a vendor that has the global infrastructure to support your performance requirements and validate that with real-world benchmarks for latency.

☐ **Expertise, especially including threat research.** 🔍

Ask questions about how long the vendor has been in the bot protection business, and whether they have the necessary expertise and experience to manage and mitigate bot threats for your organization. Do they have expertise in your industry vertical?

For example, are they experts in managing flash sales on retail sites or blocking fraud for hospitality and travel? What is their track record for analyzing and **addressing the latest threats**? Look for a vendor that devotes expert resources to research and stay ahead of bot threats, and one that has relevant experience with your industry vertical.

☐ **Peer reviews & industry recognition.** 👍

Is the vendor well-regarded by its customers and highly-rated by its users? What are customers saying about the detection effectiveness, protection performance, services, support, and user experience? What is the vendor's **Net Promoter Score (NPS)**?

What perspective do prominent industry analysts like Gartner and Forrester have? A good resource is the **G2 Grid® Report for Bot Detection and Mitigation**. Look for a vendor that is consistently recognized by companies that have deep experience with the vendor's solutions.

See how analysts with extensive client engagements have assessed the bot management solution capabilities independently.

- [ ] **Implementation track record.** 🥇

Another important metric to examine is a vendor's **track record** of successful implementations. Are customers happy with the product and its ease of onboarding and implementation in their architecture? Can the vendor provide case studies and customer referrals of successful deployments with organizations similar to yours?

The answers here can help you de-risk any new bot protection project you undertake and increase the ROI of your implementation by avoiding known pitfalls with particular vendor implementations. You should always look at other companies' feedback on a product—both positive and negative—when choosing what's right for your business.

Services & Support

- [ ] **Professional services.** 🤝

Enterprises should not need to rely heavily on services due to a product's complexity or difficulty to operate. Instead, professional services should add incremental value through specialized expertise and sharing best practices for bot protection.

Your bot management solution should come with a team of experts that are **there when you need them**—from onboarding and deployment to consultations, securing special events, and addressing custom requirements fast. In fact, the right solution will save you money in the long run, both in averted costly bot attacks and employee hours spent mitigating bots.

Most **bot management reviews** validate that threat research expertise and security operations center (SOC) support are essential to staying ahead of fraudsters' latest tactics while also being responsive to your inquiries 24/7. Look for a vendor that will help your business mitigate persistent business risk and save your teams the time they would otherwise spend manually preventing, managing, and recovering from bot attacks.

☐ **Transparent & predictable pricing**. 💰

Is the **pricing transparent** and predictable, not only at inception but also at renewal? Or is the vendor known for unexpected cost hikes? Straightforward pricing enables you to align within your budget and operational needs.

What is the total cost of ownership? Keep in mind that more resources are required to support more complex software, and ineffective protection leads to higher fraud costs.

What are the potential long-term savings with a best-of-breed solution, and how can those savings allow you to refocus your resources on more strategic projects? Look for a vendor with reasonable pricing for the solution offered. Choose a vendor and solution you are confident will mitigate your risk and vulnerability to fraud and resulting damages.

The right solution will **save your business more than it costs** in the long run.

☐ **Customer support.** 👩‍💻

When something goes wrong or questions arise, you must be able to trust that your vendor can resolve any issues quickly. Will they provide ongoing support and maintenance for the solution?

What is their response time and track record for addressing customer needs and resolving issues? Do they back that up with clear service-level agreements (SLAs)?

Good indicators here include a high customer retention rate, positive **user reviews**, and an exceptional **NPS (Net Promoter Score)**. Look for a vendor with easy-to-find customer reviews, **proven use cases**, a responsive customer support team, and clear SLAs that meet your own SLA objectives.

Use this **Vendor Comparison Sheet** to weigh all your solution options.

1. **Is the bot management delivered as a service (is it a SaaS solution)?**

   Compared to software you have to manage yourself, SaaS solutions are designed to be a **force multiplier** for your team. Your solution should come with easy installation, a **broad selection of integrations**, onboarding assistance, and dedicated customer support teams to answer your questions and keep your protection up to date.

   Avoid software-based bot protection that your team has to deploy, manage, scale, and troubleshoot, which quickly becomes a **drain of resources**, adding operational costs and extra complexity to your security stack. Software-based tools tend to be based on **legacy WAF** technologies.

   Peace of mind is essential to your team's ability to focus on business-driving activity. Choose bot protection equipped with a specialized team you can trust to step in and keep your business and consumers safe during an attack.

2. **Does the solution provide real-time, at-the-edge bot protection and analyze every request, every time?**

   When it comes to the online user experience, you know that every millisecond counts. Your bot protection should be able to review every request anew, at the edge, *when the request is made,* rather than reviewing requests later (after threats have already accessed your website, app, or API).

   Another imperative capability is **instant**, **AI-powered** **aggregate global detection**, or a solution's ability to immediately and continuously update its ML detection models based on the collective intelligence gathered from all protected endpoints, worldwide. With instant aggregate global detection, a new threat signal detected on one customer endpoint is instantly shared across all customers and endpoints.

   For an advanced bot and online fraud solution that processes trillions of signals per day, the value of collective intelligence cannot be overstated.

3. **What is the false positive rate?**

   When a bot management vendor processes millions of requests (or more) every day, there is a chance that some human requests can get mistakenly flagged as bot requests. But a smart goal is to **preserve your user experience** (UX) by ensuring that **as few human users as possible** get blocked or challenged with a CAPTCHA.

   Therefore, one key metric for detection accuracy is the **false positive rate**, which measures the percentage of actual human requests the detection system challenges as suspected bots. Effective bot management solutions strive to minimize their false positive rate, and provide you with transparency about what it is.

   Some bot management vendors suffer from false positive rates as *high as* ***0.75%***, which may not sound high, but is well above the ideal false positive rate of 0.01%. A higher false positive rate adds more friction to your UX. But dialing back the sensitivity allows sophisticated bots to evade detection. Inaccurate bot detection can also result in many negative consequences beyond a poor UX and security risks, such as increased fraud costs and reputational damage.

   In addition to keeping the false positive rate low, advanced solutions will prioritize a **feedback loop** to constantly improve detection models based on accuracy and performance metrics like the false positive rate.

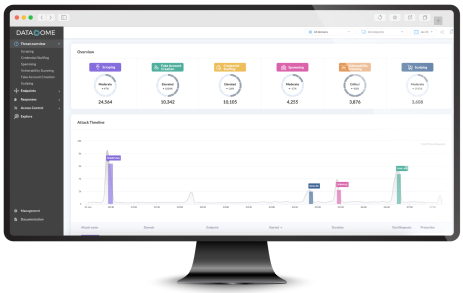
4. **Is the solution easy to deploy on your architecture?**

   You don't want to have to rely on the availability of your vendor's professional services team to hit your project timelines. If bot protection takes days or weeks to onboard and requires custom integrations or complex deployments, it leaves your business exposed for fraudsters to exploit longer.

   Integrations with your infrastructure should be quick and easy to reduce your vulnerability and protect your team's time. Look for a **well-documented solution** that:

   - Can be implemented in minutes.
   - Includes standard integrations with cloud and CDN providers.
   - Offers an extensive set of client-side, server-side, and third-party integrations with technology partners.
   - Is available in public cloud marketplaces.

5. **Are the dashboards and user interface easy to navigate?**



Being able to get real-time threat information and set the protection you need fast is critical. Avoid sifting through several reports and pages or sitting through weeks of software training to get the information you need.

You should get easy access to a **real-time view** of all your incoming requests and web traffic, including the threats attacking your website, app, and API—at a glance, as well as different, more detailed views.

Look for the ability to examine specific events, quickly drill into relevant information, and view your traffic by attack type, user, account, trend, and other views that help reveal patterns and useful insights. You may also want to inquire about a mobile app companion to see attack alerts and explore traffic information on the go.

6. **What are the reporting and analytics capabilities?**

In addition to a user-friendly dashboard, your solution should provide various reports and analytics your team can drill into if needed. The right analytics will help you quickly gain insights from a complex data set.

Custom reporting is an important capability that can allow you to easily generate and share relevant information with key stakeholders across your organization. In contrast, subpar reporting can become time-consuming for your team to support.

7. **Does the protection support the optimal user experience for your human customers?**

A great user experience (UX) for your customers is paramount to keeping your business running smoothly. Therefore, your bot management should **not** rely heavily on CAPTCHA challenges as the primary protection mechanism or first line of defense.

Instead, a comprehensive bot solution will provide a **frictionless experience**, only showing CAPTCHAs to suspected bots based on the perceived risk level.

The perceived risk should be based on the solution's analysis of many diverse detection signals, prior to ever showing the user a CAPTCHA.

The **CAPTCHA** should only be presented after a user is flagged as suspicious based on many sophisticated signals. Therefore, only if the detection accuracy is flawed will your consumers see CAPTCHAs more frequently.

To preserve your UX, you need a solution that learns and optimizes detection in real time using a multitude of signals, including user behavior and (only when appropriate) CAPTCHA response. Traditional CAPTCHAs that operate in a silo and rely on the difficulty of a challenge to identify and block bots are no longer effective.

8. **Does the detection use both server-side and client-side signals?**

Bots are evolving by the second, so detection must rely on a variety of signals from many sources to root out malicious actors. Both server-side and client-side signal collection are **required** for efficient and effective bot detection.

Server-side detection is great for simple bots with suspicious HTTP and **TLS (Transport Layer Security) fingerprints**, but to identify today's sophisticated bots, more signals are required. Client-side detection helps with browser, app, and user event tracking to detect advanced bots that masquerade more effectively as humans.

Some bot management tools on the market are limited to either client-side or server-side detection, and some only gather very limited signals from one side or the other. The key is to make sure you have options (both client-side and server-side data) to maximize effectiveness and meet future needs.

9. **Does machine learning (ML) drive the solution to keep it ahead of threats on autopilot, and if so, how are the ML models maintained?**

Bad actors and fraudsters have easy access to AI, bots as a service, residential proxies, and more sophisticated tools by the day to bypass stagnant security software. Therefore, bot protection requires advanced ML technology to stay ahead of ever-evolving attacks.

With ML, advanced bot protection can operate on autopilot, processing and responding to every request in real time, and requiring no manual intervention or maintenance from your team. ML helps organize data and improve prediction accuracy—empowering advanced solutions to detect even never-before-seen threats.

Because malicious bots are created and used for many different purposes using various shifting techniques, effective bot detection requires multiple ML models to ensure **accuracy without compromise**. Perhaps most importantly, the ML models must be **monitored by dedicated threat research experts**, who can train and test them regularly, and can always intervene if needed.

10. **Is the solution monitored by a dedicated threat research team?**

Only a dedicated threat research team and SOC (security operations center) can ensure your protection continues to respond with unparalleled accuracy and flexibility. A team of full-time experts can constantly follow and analyze the latest hacker tools and deploy protection against them **before** malicious actors reach your platform.

Having a **24/7 threat research team** to monitor, update, and optimize your solution's detection models, as well as creating custom rules as new threats arise, is essential for true peace of mind.

Get all the details you need with this **RFP Template**.

Conclusion

Bot protection is the foundation of online fraud prevention. Thus, it's no surprise that advanced bot and online fraud protection has become a strategic focus for many cybersecurity leaders. It is critical for online businesses to prevent scraping, account takeovers, payment fraud, and other detrimental attacks that get cheaper and easier for fraudsters to automate each day.

To mitigate your risk of fraud, data breaches, downtime, reputational damages, and countless other consequences, now is the best time to implement a sophisticated and specialized bot management solution that will help **stop fraud before it starts**.

How you prioritize the criteria outlined in this buyer's guide in your decision-making process depends on your enterprise's biggest pain points and priorities. Your next step should be to choose the solution that addresses your most urgent pain points and organizational priorities while also solving potential future use cases.

To make your most confident decision, **measure and test** your shortlist of bot management solutions in a real-world environment. You can trial solutions independently, or install one vendor alongside another to identify the differences and discrepancies in detection. You can also hire an external company (or use a bot-as-a-service platform) to conduct a pentest targeting your priority endpoints that need protection.

Fraudsters will continue to target enterprises, always increasing the quantity and effectiveness of their attacks. They will persist in attacking the most popular endpoints (from account creation to login and checkout) across your mobile apps, websites, and APIs. **Be ready.**

More Tools for Your Search

- **Vendor Comparison Sheet**: Your spreadsheet to fill in and weigh all your solution options (including DataDome 😉) in one place.
- **RFP Template**: This thorough, editable RFP document is for you to use with your vendor(s) of choice.
- **Internal Solution Pitch Template**: A presentation deck you can use to get all your organization's key stakeholders on the same page for fraud prevention.