HUMAN

Bot Management in the Era of AI— A Buyers' Guide

Bot Management in the Era of AI —A Buyers' Guide

Table of Contents

1.

Introduction: Why Bot Management Is Critical for Organizations

The Rise of Digital Deception and the Growing Importance of Protecting Customer Trust

The digital world is no longer human by default. The use of automation by both basement hackers and sophisticated cybercriminals is scaling faster than ever, eroding digital trust and putting businesses at risk. Fake accounts, synthetic traffic, and fraud are becoming more deceptive and challenging to detect—and more costly to ignore.

The lifecycle of digital attacks and fraud often involves both automated and human activity. Fraudsters are increasingly blending bot attacks with fraudulent human behavior to commit account fraud and other abuse. Because of this, today's threatscape demands more than traditional tools that simply catch the obvious signs of automation, such as rapid-fire login attempts, basic scraping, and crude attack patterns. Security and fraud teams must go beyond basic bot detection to differentiate between good and bad bots and authentic and fraudulent human activity across their customers' entire digital journey—as users search, shop, stream, and socialize online.

Furthermore, attackers are exploring AI tools as an accelerant to evade detection. Large language models (LLMs) and AI agents blur the line between human, good bot, and bad bot. Legitimate consumers use chatbots, price comparison tools, and agentic AIs to navigate the digital world and interact with your organization online. This means the challenge isn't just blocking sophisticated threats; it's gaining complete visibility into the behavior and intent of AI agents to help you make strategic and security decisions that protect your customers and your business.

The New Era of Bot Management

In the past, bot management has been reactive, fragmented, and narrowly focused on blocking bots without considering the broader impact. But it is no longer simply about security—it's about trust, authenticity, and transparency. This requires a proactive and strategic approach.

Then	Now
Prioritizing blocking bots while ignoring downstream human-led threats, leading to higher fraud losses.	**Prioritizing digital trust** by ensuring real customers can engage seamlessly while stopping automation with malicious intent.
Detecting bot-or-not and differentiating between "good" vs. malicious automation.	**Detecting individual bot profiles**, identifying what action each specific bot is taking to determine its intent.
Static detection methods that do not follow through the entire attack lifecycle beyond automation—and that cannot keep pace with adapting sophisticated threats.	**Adapting through the full lifecycle of cyberfraud** by detecting malicious human activity and continuously learning from attacks to stay ahead adversaries.
Bot management as a cost center without recognizing the ROI generated by proactively stopping fraud and building long-term consumer trust.	**Bot management as a business enabler** to prevent fraud, reduce friction, and enhance user experience.
Security, fraud, and identity teams working in silos, causing operational inefficiencies and slower threat detection and response.	**Breaking down silos between security, fraud, and identity teams**, allowing for faster, more coordinated responses to evolving threats.

Navigating the Bot Management Software Market

As automated threats have become more sophisticated and deceptive, the vendors offering mitigation solutions have also proliferated. Buyers are left to sort out the difference between solutions and determine which one is right for their organization. This guide is an educational resource to help security and fraud practitioners filter through the noise and zero in on the criteria that matter for both security and customer trust.

This guide will help buyers understand:

- The evolving bot landscape and what's at stake today
- How bot threats are shifting—and what to expect tomorrow
- Key criteria for evaluating modern bot management solutions
- How to position bot management as a strategic advantage, not just a security measure

The fight against bots is no longer just about blocking automation—it's about preserving digital trust in a world where the line between human and machine grows blurrier every day. In the following sections, we'll outline the key considerations that should influence your assessment to determine the right bot management solution for your unique needs.

It's All in the Data

Organizations often operate in silos, but fraudsters don't. Modern bot attacks are interconnected and follow consumers throughout their digital journey—as they click on a digital ad, browse an application, log into an account, and enter payment information on a payment checkout page. There are ample opportunities for bad actors to capitalize on the gaps in protection coverage by committing numerous types of attacks via automated attacks and human-led fraud spanning from ad fraud to account takeover.

The only way to defeat interconnected cybercrime is with interconnected data. That means capturing signals from user interactions across advertising, application, and account surfaces. By leveraging machine learning models trained on a diverse and extensive data set, bot management solutions enable organizations to feel confident in high-fidelity decisions that differentiate between legitimate and illegitimate activity.

Conversely, solutions that only collect signals at disparate touchpoints lack integrated and adaptive feedback loops. Tools that solely look at edge traffic or focus on narrow use cases cannot match the accuracy of a comprehensive approach. Only a vendor with visibility across multiple interaction points can effectively protect against sophisticated bot attacks and digital fraud.

A platform approach, built on a large and diverse data set of threat activity, enables organizations to follow the behavior of bad actors over time—from the very first interaction with a website or app, through to the day-to-day usage of accounts. By analyzing signals from touchpoints throughout the customer journey, solutions can provide unified, comprehensive detection and mitigation.

2.

Understanding Kinds of Bot Attacks

Bad actors use malicious bots to execute a number of attacks to exploit or disrupt applications and users.

Bots 101

What Is a Bot?

A bot (short for "robot") is a software script or program designed to perform automated tasks. Bots are programmed to execute specific. actions quickly and efficiently, often mimicking human behavior to interact with users, systems, or other programs.

Are All Bots Malicious?

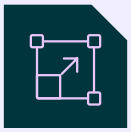
No. There are many types of bots that can be beneficial to organizations. "Good" bots perform useful functions and automate repetitive tasks. However, bots can also be used by bad actors to engage in malicious or unethical behavior that harms users, businesses, or systems for personal gain or disruption.

Why Do Cybercriminals Use Bots?

Bots have several qualities that make them the weapon of choice for cybercriminals. These include the following:

Automation
Bots perform tasks without human intervention.

Speed
Bots execute tasks faster than humans can.

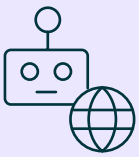


Scalability
Bots can handle repetitive tasks at scale, making them ideal for managing large workloads.

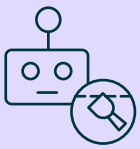
Specialization
Bots are designed for specific purposes, such as chatting, searching, or monitoring —or attacking a specific application.

Examples of Common Bot Types

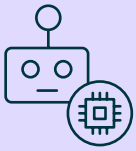
Chatbots
Simulate human conversations (e.g., customer support, personal assistants)



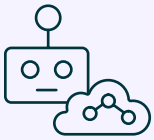
Web Crawlers
Index websites for search engines



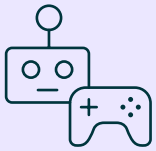
Scrapers
Hoover up content from websites, increasingly driven by the need to fuel AI/LLM models



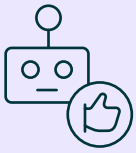
AI Agents
Operate with some degree of autonomy, making decisions, taking actions, and adapting over an extended period of time



IoT Bots
Interact with smart devices

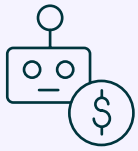


Gaming Bots
Enhance game play or simulate players

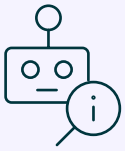


Social Media Bots
Automate activity on social platforms (e.g., likes, comments)

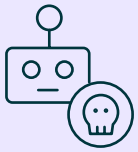
E-commerce Bots
Automate shopping or price tracking



Trading Bots
Execute financial trades automatically



Monitoring Bots
Track events or changes (e.g., website uptime, weather)



Malicious Bots
Perform harmful activities (e.g., spamming, distributed denial of service [DDoS] attacks, credential stuffing, carding)

Attacks Targeting Accounts

Account takeover

Account takeover is a form of fraud in which cybercriminals gain unauthorized access to online accounts. Attackers use bots to launch account takeover (ATO) attacks in several ways (including credential stuffing, credential cracking, and password spraying) and then use the compromised account to carry out fraud, like transferring funds or using stolen credit cards. According to The Quadrillion Report, ATO attacks make up more than 20% of all login requests.

Consequences of ATO attacks

Financial losses

Once an attacker has compromised an account, they can transfer funds, make purchases with stored credit cards and gift cards, steal stored personally identifiable information (PII), drain loyalty points, sell or transfer airline miles, and distribute malware, among other types of fraud.

Reputation damage and loss of consumer trust

ATO attacks can erode consumer trust, especially if users are locked out of their accounts or if funds or PII are stolen. Security incidents can also result in negative press.

Increased resource costs

Attack investigation and remediation can require significant support from IT, security, and customer service teams.

Fake account creation

Cybercriminals use bots to create fake accounts en masse using bogus or stolen identity information.

Consequences of fake accounts

Financial losses

Fake accounts can abuse sign-up offers, loyalty programs and other promotions, test stolen credit cards and fraudulently apply for credit.

Reputation damage and loss of consumer trust

Fake accounts can spread misinformation (AI tools have made it easier for bad actors to create realistic-looking comments at scale), distribute spam and malware, send phishing emails, and otherwise make it difficult for businesses to build and maintain authentic relationships with their customers.

Skewed analytics

Fake accounts can influence website metrics, leading to wasted resources and ineffective marketing campaigns.

Attacks Targeting Applications

Scraping

Scraping is the technique of using bots to extract content or data from websites. There are many legitimate scraping bots, such as search engine crawlers, ad verification bots, and content categorization bots. Bad actors can also use scraping bots for more nefarious purposes, including price scraping, content scraping, and data harvesting. LLMs have increased the demand for and accessibility of scraping, both for the purpose of training the model and delivering or summarizing content in response to a user prompt.

Consequences of scraping attacks

Loss of competitive price advantage

Competitors may use scraped information to create counterfeit products or adjust their pricing strategies to undercut your business.

Skewed analytics and infrastructure strain

Large-scale scraping operations can artificially inflate website traffic, making it difficult to glean accurate insights from data. High volumes of scraping requests can slow down websites and even cause outages.

Content revenue loss and reputation damage

Scraping may result in people consuming your content without visiting your website, either on another site that has reposted your content or within an AI platform. Scraping raises concerns of plagiarism and intellectual property infringement, especially if scraped content is reposted on other websites.

Transaction abuse

Transaction abuse takes place when bots are used to attack your checkout flow. Carding is one type of attack in which malicious actors attempt purchases with stolen credit cards in order to validate them. Scalping and inventory hoarding are other examples. These describe the practice of snatching up large quantities of products online, either to purchase and resell or to hold in online carts.

Consequences of transaction abuse

Financial losses

If carding attacks are successful, the business might have to refund fraudulent purchases and pay chargeback processing fees. Scalping of hot products (like video game consoles) causes businesses to lose out on the sale of companion products (e.g., video games).

Eroded consumer trust

Customers may feel dissatisfied and upset if bots deplete inventory before they can buy it.

Loss of competitive advantage

Stockouts may cause customers to shop elsewhere and turn to competitors for future purchases.

Data contamination

Data contamination describes how both wanted and unwanted bot traffic can skew web metrics and engagement data, impacting data-driven decisions. This includes bot-generated invalid traffic (IVT), fake likes, comments, and reviews, and spin fraud.

Consequences of data contamination

Reputation damage and loss of consumer trust

When bots spread misinformation or fake engagements, it is difficult for businesses to build and maintain authentic relationships with their customers.

Wasted marketing spend

Skewed engagement metrics may influence campaign and targeting decisions in the wrong direction.

Spin fraud losses

Businesses may lose money on fraudulent royalty payments or share of ad revenue.

Layer 7 DDoS

Layer 7 distributed denial-of-service (DDoS) attacks target the application layer in the OSI model. This kind of attack is an attempt to overwhelm application server resources with a flood of traffic (typically HTTP traffic). These can slow site performance and cause a service disruption.

Consequences of Layer 7 DDoS attacks

Customer dissatisfaction

The negative performance impact may result in poor user experience, and frequent DDoS attacks could lead to reputation damage.

Financial losses

If customers are unable to use the service, this prevents organizations from generating revenue during a DDoS attack.

Data breach risk

A Layer 7 DDoS attack can be used as a cover to exploit vulnerabilities and gain unauthorized access to sensitive data.

What Is Business Logic Abuse?

Business logic abuse describes a cyberattack that exploits an application's intended business rules and processes. Examples include when a user creates numerous accounts so that it can repeatedly receive a signup offer, exploiting referral programs to gain excessive credits, or logging into someone else's account using valid but stolen credentials. By manipulating legitimate features, attackers can achieve unauthorized outcomes while appearing to use the application normally. Cybercriminals may abuse a website's business logic to carry out many types of attacks.

Attacks Targeting Advertising

Click fraud

Click fraud is the deliberate practice of generating fake clicks on digital advertisements, typically through automated bots or human click farms. This deceptive activity can come from various sources, including competitors trying to drain advertising budgets, dishonest publishers attempting to increase their revenue, or sophisticated criminal operations. By simulating genuine user engagement, these fraudulent clicks make ads appear more successful than they actually are.

Consequences of click fraud

Wasted advertising spend

Businesses may spend money and resources on generating and following up with fake clicks that will never convert to actual customers.

Skewed analytics

Click fraud influences campaign data, leading to misguided optimization decisions.

Decreased trust and reduced value

Organizations may lose trust in legitimate advertising platforms and publisher networks, impacting future investment decisions and hurting genuine publishers and platforms.

Programmatic ad fraud

Programmatic ad fraud occurs when bad actors exploit automated advertising systems to steal advertising budgets. These fraudsters create fake inventory, generate fake impressions, and misrepresent where ads appear. Common tactics include domain spoofing, bot traffic, and ad injection.

These deceptive practices undermine the transparency and effectiveness of programmatic advertising, making it harder for advertisers to trust the automated buying process.

Consequences of programmatic ad fraud

Financial losses

Ad spend may be directed to nonexistent or misrepresented inventory.

Corrupted performance metrics

Corrupted performance metrics distort campaign optimization and planning.

Loss of trust

Ad fraud damages industry confidence in programmatic buying and selling and erodes trust between buyers, sellers, and technology platforms.

3.

How to Know If You Have a Bot Problem

Bot attacks can be executed on web and mobile apps and application programming interfaces (APIs). There are a few basic warning signs that can serve as potential indicators that you have a bot problem.

Hundreds or thousands of login or checkout attempts

This kind of activity can indicate that a credential stuffing or carding attack is taking or has taken place.

Inhuman user behaviors

Simple bots scroll sites more quickly and precisely than humans do, though it is important to note that sophisticated bots mimic human behavior.

Spikes in password reset requests

After fraudsters take over an account, they immediately change the password.

Spikes in help desk calls

Consumers will likely contact customer support if they are notified of an unauthorized login to their account or if they are locked out of their accounts because of an unauthorized password change.

Unusually high numbers of chargeback requests

This kind of activity can indicate someone is buying with an unauthorized account.

Spikes in shipping address changes

This can indicate an account has been compromised by shipping fraud, where criminals use drop-shippers (entities that sell products that aren't in stock) or mules (accounts for money laundering) to forward illegal purchases.

Spikes in average purchase item price

Criminals often buy expensive items to make more money with fewer purchases to reduce the risk of being discovered.

Multiple, rapid-fire changes to accounts

This is a major red flag of account fraud. Users rarely need to change their payment information, address, and password at the same time.

Spikes in reward points activities

Fraudsters redeem bonuses for merchandise or services, drain them to sell on the dark web, or add them to their accounts.

Anomalous IP patterns

An increase in IPs associated with multiple devices, multiple accounts, or pointing into untraceable ranges can indicate that a fraudster is manipulating IPs.

Slow application response time

Some bot attacks unleash large numbers of requests that overwhelm your application and congest your content delivery network (CDN).

4.

Seven Key Criteria for Choosing a Bot Management Solution

When embarking on your journey to purchase a bot management solution, there are six key criteria that should remain top of mind.

1. **Efficacy**

2. **Impact on performance and user experience**

3. **Fraud monitoring and mitigation actions**

4. **Ease of deployment and ongoing maintenance**

5. **AI agents and "good bot" management**

6. **Dashboards and reporting**

7. **Platform capabilities**

Let's break each of those down.

1. Efficacy

Efficacy is the most critical factor in choosing a bot management solution. If bot attacks aren't accurately detected and mitigated, nothing else matters.

At first glance, it can be overwhelming to sort through various vendors' solution materials that all make similar, if not identical, claims. We recommend focusing on the following to simplify your efficacy research.

Questions to ask about efficacy:

How well does the solution adapt to changing attack techniques?

Look for tools that can detect and mitigate the most sophisticated and determined adversaries, using behavior- and signature-based machine learning (ML) models, device fingerprinting, and artificial intelligence (AI) that adapts based on your specific threats.

Does the solution analyze every interaction?

Look for tools that continuously analyze every interaction from a user and update decisions in real time — not only when a request hits your server. The solution should also examine every action taken in an account to assess whether the right person is using it.

Does the solution stop at the bot-or-not decision?

Look for solutions with secondary detection capabilities (see definition below) that sort through vast amounts of data post-decision to profile attacks and automatically optimize mitigation strategies over time as threats evolve. When it comes to accounts, look for a tool that can also answer "is this the right person?" and "are their actions legitimate?"

Does the solution use defense-in-depth strategies?

Look for solutions that provide layered defenses, with pre-login credential monitoring, at-login bot mitigation, and post-login activity analysis all being critical components. And choose a vendor that takes a network approach to bot mitigation, where a detection event on one customer strengthens protections for every customer.

Does the solution detect and stop AI-driven attacks and other emerging threats?

Look for tools that leverage adaptive detection technology to track and block new and existing threats as they change over time, such as agentic AI, ensuring a continuous line of sight and continuous protection. Focus on solutions with robust anti-tampering mechanisms that cannot be beaten or reverse-engineered by AI. Ideally, your chosen vendor should also help to control AI-related traffic and enable the monetization of content that is being targeted.

What are customers and analysts saying?

Read reviews and reports, such as G2's seasonal grid and The Forrester Wave™: Bot Management Software, Q3 2024, to get perspectives from your peers and trusted analysts.

What Is Secondary Detection?

Secondary detection refers to the use of advanced technology to analyze data and identify threat patterns after an initial decision is made. In bot management, this means looking beyond a single bot-or-not decision to review attack data in aggregate. By comparing each attack with everything that happened previously, analysts can uncover hidden threat patterns and zero in on the attacks that matter—which, in turn, accelerates investigations and threat response.

2. Impact on performance and user experience

When users become frustrated and abandon an application because of performance issues, the solution loses its value.

There are two essential considerations: latency and end-user friction. Latency describes the impact on site performance, and friction refers to disruption of user experience. On both counts, a solution must be fine-tuned to meet the specific needs of your business and unique infrastructure environment.

Questions to ask about latency:

Does the solution prioritize a low-latency experience for human website visitors?

Consumer satisfaction is key, so vendors must ensure that only bots—not real humans—experience high latency.

Are slow and expensive server-to-server calls executed on every request without your control?

Advanced technology can pre-validate human users and analyze every interaction asynchronously without conducting a server-to-server call each time a request is made.

Can you configure the solution to influence latency depending on your specific risk parameters?

Customizable solutions will allow you to adjust the balance between detection tolerance and friction so you can find the level that works best for your business.

Questions to ask about friction:

Does the solution use a third-party CAPTCHA (like reCAPTCHA) to challenge human website visitors?

If your solution relies on a third-party tool, the third party owns the CAPTCHA solve data—meaning the bot management solution is missing out on critical signal to support adaptive learning. Furthermore, research has shown that many standard CAPTCHAs don't deter sophisticated bots while adding unnecessary friction to the customer experience.

How often are CAPTCHAs shown to human website visitors?

Solutions that analyze user interactions in the background can pre-authorize human users, ensuring that only risky requests are presented with a CAPTCHA. This provides detection accuracy while preserving an uninterrupted consumer experience.

Does the solution offer a low-friction way to verify humanity?

Using a simple press and hold button that runs tests behind the scenes is less frustrating and more effective than a complicated puzzle or game.

Is there an adaptive learning feedback loop?

Make sure the data collected from CAPTCHA solves is actively improving your detection. No solution is bullet-proof, but the best solutions are actively learning from user feedback in order to continuously optimize detection and minimize friction on real users.

Is the solution robust against AI captcha solvers?

Studies have shown that commercially available AI tools have a 100% solve rate on puzzle or visual-based challenges. Leveraging robust anti-tampering mechanisms will make it difficult to solve CAPTCHAs through automation, AI, API calls, or CAPTCHA farms.

Does the solution pre-filter bad bots without requiring users to solve a CAPTCHA?

Instead of challenging every request, look for solutions that can block bots on the first request, before they hit your site. This provides an even lower-friction experience that does not require any interaction from the end user.

3. Fraud monitoring and mitigation actions

Online user accounts are ripe targets for fraud—by both bots and human fraudsters. Because of this, it is necessary to leverage a range of detection mechanisms and mitigation actions to stop fake and compromised account fraud in each unique scenario.

Questions to ask about fraud monitoring and mitigation actions:

Can the solution monitor actions taken within an account and identify patterns of fraud?

The chosen solution should be able to go beyond "human or bot?" and answer "is this the right human?" and "are these actions legitimate?". Post-login monitoring that assesses each action taken within an account is key.

Does the solution offer a combination of sophisticated detection techniques?

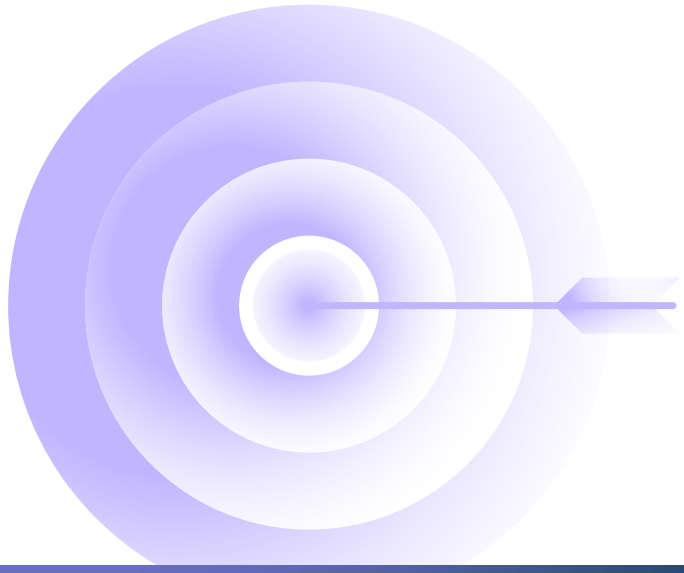
Key features and capabilities include identifying groups and clusters of shared accounts (multiple accounts controlled by a single actor), velocity (where a repetitive behavior deviates from 'normal' activity levels), profile deviation (e.g. logging in from a new country and new operating system), behavioral analysis (e.g. active at different times of day or changes to normal activity), flow-based detection (where a sequence of activity indicates fraudulent behavior), and reputational analysis (e.g. disposable email, VPN/Proxy/TOR IP).

Is intelligence on compromised credentials offered?

Credential stuffing attacks are one of the most common attack vectors used by bad actors to commit account takeover attacks. Look for a solution that actively monitors compromised credentials in the wild.

What mitigation actions are available within the solution?

When it comes to mitigation options the customer really must be king, so a choice of default actions and API integrations that allow customization is key. Stopping bots hitting websites and apps with a straightforward block is usually default, but some organizations may prefer to display alternative content depending on their use case. With online accounts, organizations may wish to send password reset emails if compromised credentials are identified. If fraudulent activity is flagged in an account, they may wish to lock the account, flag it for review by their fraud team and create a ticket for their support team in case of a helpdesk call.



4. Ease of deployment and ongoing maintenance

Buyers should consider solution architecture and identify where it sits within existing infrastructure, including integrations with your cloud delivery network, load balancer, cloud platform, and so on.

Consider this from both a desktop and mobile perspective. If your organization has a mobile application, choosing a solution with a mobile software development kit (SDK) is critical to protect mobile traffic. The same applies to hybrid apps and other operating systems like visionOS.

When it comes to ongoing maintenance, you'll want a tool that works without requiring extensive configuration from your security or fraud team, but also gives you control to modify and refine on an ongoing basis. The best solutions function on their own and are easy for customers to manage independently. However, having a strong customer support team at the ready makes all the difference, so it is important to consider the level of support your business needs from the vendor.

Questions to ask about deployment and maintenance:

How will the solution integrate with my existing environment?

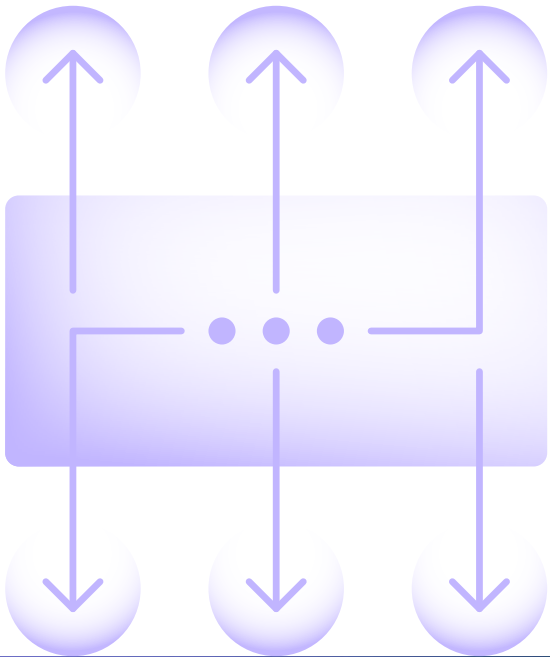
Look for solutions that will integrate seamlessly with your existing environment, such as your CDN, web server, cloud platform, CIAM or SIEM systems.

Is the solution deployed on the client side or the server side?

Deploying a solution with both client-side and server-side components ensures maximum signal is collected on each user. Every bot management solution that has blocking capabilities uses a server-side component to analyze the request. Specialized solutions also have a client-side component to monitor user behavior (e.g., mouse movements, keystrokes, and other user interactions). Only relying on server-side means that user activity data is not analyzed, which results in lower detection accuracy.

Does the solution have a mobile SDK? Does it support hybrid apps?

A mobile SDK allows organizations to collect more signals and enforce more aggressive detections on risky profiles. Without an SDK, it's impossible to serve a CAPTCHA to app users. This means that the only option is hard-blocking all suspicious mobile users, which risks blocking real customers. In addition, not all mobile SDKs fully support hybrid applications. It is important to qualify this with your shortlisted vendors if you are running hybrid applications.



What resources will be required to manage this solution on an ongoing basis?

Look for a vendor that continuously performs risk threshold and scoring optimization while also allowing you to make adjustments yourself if you so choose. The goal is to achieve collaboration between the system's intelligence and human analyst expertise.

How is the vendor's customer support?

Select a tool that offers flexible options for working with support, including communications channels, response SLAs, and additional services. Customer reviews, such as G2's seasonal grids, are also a great source of input on the quality of a vendor's service team.

The Bot Management Balance

In an effort to deliver ROI, it is easy to place a premium on certain criteria above all else. While things like speedy onboarding or low cost may seem attractive, there are often trade-offs that may be overlooked. Here are some common traps:

Onboarding speed

While rapid onboarding is of course a huge plus, it must be balanced against other considerations. For example, web application firewall (WAF) or content delivery network (CDN) add-on solutions may offer the quickest onboarding, but the resources required to manage them may overshadow the initial time saved. Furthermore, add-on solutions often lack the specialization needed to mitigate sophisticated bots and dedicated attackers.

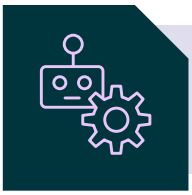
Solution cost

With cost containment pressure mounting, it may seem wise to choose low-cost solutions across the board. However, if the solution has less sophisticated detection capabilities, lower efficacy, and is more resource-intensive to manage, you will not realize a positive ROI. Assess the resource impact and service-level changes that are associated with reduced upfront costs to make sure you don't end up paying more on the back end.

Self-service

Some customers may initially opt for seemingly simple check-box and plug-and-play bot solutions often tied to CDN and WAF vendors. However, these solutions can be burdensome to self-manage. The promise of effortless efficacy often needs to be revised due to constraints required for continuous tuning, monitoring, and management.

Weighing various criteria appropriately is critical to ensure a long-term bot defense strategy that addresses your unique security challenges.



5. AI agents and "good bot" management

Not all bots are malicious. Some bots—such as search engine crawlers, ad verification bots, and monitoring tools—are necessary for a business to operate. When it comes to good bot management, visibility and control are just as important as detection.

AI Agents that scrape or summarize content are prime examples. The ability to choose how to manage these bots is increasingly becoming more critical as AI continues to become more pervasive.

Questions to ask about AI agents and good bot management:

Does the solution provide visibility into known bots and AI agents?

Choose a solution that detects known bots and AI agents and provides insights into their traffic patterns, including a granular breakdown of which bots are targeting which paths and accessing which content—so you can make informed decisions to protect your assets and maximize your content's value.

Can your organization customize responses to known bots and AI agents?

Select a tool that enforces robots.txt directives for both known and unknown bots using powerful, granular policies to prevent unauthorized content scraping or summarization. A vendor should manage a tailored list of known bots with out-of-the-box and customizable response policies to allow, block, or request-limit traffic, time-box response policies during busy periods, and show alternative content if desired.

Does the solution provide visibility to identify and track AI agents over time?

Choose a solution that uses a detection feedback loop with adaptive learning to continuously track and label AI agents across your content and properties, enhancing detection and response time. As legitimate humans increasingly use AI tools to interact with organizations online, digital businesses need complete visibility into the behavior and intent of AI agents on their applications.

How will you minimize invalid traffic (IVT) and protect brand reputation?

Look for a solution that blocks unwanted scraping bots to minimize IVT and prevents unauthorized reposting of your content while allowing paying AI agents to access your content ad-free. This will help ensure your brand integrity remains intact.

Does the solution protect against AI-generated cyberthreats?

Adopt a solution that is equipped to mitigate fraud driven by the malicious use of AI, as well as AI-generated manipulation that distorts engagement, drains revenue, and erodes trust along the customer journey.

6. Dashboards and reporting

Implementing a solution with an advanced decision engine that blocks bad bots with high fidelity is critical and necessary. Having that solution serve as a data-centric, machine learning-driven analyst tool takes bot mitigation to the next level.

Together these capabilities enable an organization to identify trends, optimize cybersecurity strategies, and stay ahead of attackers over time as they adapt and evolve their techniques.

Questions to ask about dashboards and reporting:

Does the solution surface insights from additional data analysis that takes place post-decision?

Choose a solution that mitigates attacks as they come and provides actionable analyses. Use context-driven investigation tools powered by purpose-built AI models to enrich your investigations and help you understand exactly what is happening with automated traffic on your application surface.

Does the solution report on attacker profiles and characteristics?

In addition to providing details about traffic spikes, your bot management dashboard should arm you with information about the specific types of bots targeting your application, their characteristics, and the actions taken by each one (see "What Are Attack Profiles" on page 21). Automatically correlating the disparate bot activity will help you understand the scale of attacks and identify threat patterns.

Does the customer console provide actionable reports?

Make sure the vendor console is intuitive to navigate, with different attack-type dashboards, detailed attack profiles, and out-of-the-box and customizable reports for key stakeholders.

Do vendor dashboards help jump-start and inform your investigations?

Look for solutions that provide insight into the individual attacks and constituent threat vectors that comprise a larger traffic spike, so you can discover low-volume but potentially dangerous attacks that would have otherwise remained hidden. This will enable you to understand patterns of abuse faster, prioritize investigations, and hit the ground running on incident analysis.

Content Monetization

AI-driven content scraping is posing a significant threat to publishers. In the process of creating and summarizing content, generative AI platforms rely on extensive automated scraping from entities across the web. For content-driven digital platforms, scraping by AI agents is often unwanted at best—and copyright infringement at worst.

Bot management solutions can help organizations control AI-driven content scraping, enabling security teams to view, manage, and block AI bots if desired. Analysts can dig in to understand which bots are accessing your content and what paths they are targeting, allowing you to monitor impacts and make informed decisions to protect your assets.

Some solutions are taking this even further, enabling monetization policies for automated AI agents that require them to pay for content access. When an AI agent is detected, you can execute response actions depending on payment plan or other conditions. This allows you to both block unauthorized AI agents and generate a consistent revenue stream from authorized AI partners.

What Are Attack Profiles?

An attack profile is the set of capabilities, characteristics, and actions of a specific attacker. Having data on each individual threat on your application allows security teams to break through the noise and zero in on the attacks that matter.

Analysts can jump straight into investigations to understand exactly what bad bots are doing, their sophistication, their capabilities, and the specific characteristics that distinguish them from other humans and bots on the application. This enables teams to form a threat narrative that can be shared with key leadership stakeholders and board members. This saves hours of analysis and gives customers access to uncover hidden insights that were not visible before.

Benefits

By surfacing attack profiles, bot mitigation technology serves as both a bot blocking solution and a data-centric, machine learning-driven analyst tool. Security teams can get a line of sight into the attacks that matter, which enables them to do the following:

Focus and accelerate investigations

Turn hours of exploratory analysis into a quick, focused examination of contextualized data on distinct bot activities, attack paths, and changing behaviors.

Transform attack data into a board-ready threat narrative

Easily tell your bot attack story to key stakeholders and showcase the impact of your team's work.

Make strategic decisions based on your unique threats

Optimize your security strategy for the specific threats you face with unprecedented clarity on each attacker's actions and intent.

How attack profiles work

Attack profiles are built by analyzing malicious traffic and comparing it to all past and present traffic. Purpose-built AI models analyze the attributes of all the malicious requests on an application and group those requests into distinct profiles based on attack characteristics and actions.

7. Platform capabilities

Bad bots target application, account, and advertising surfaces.

Organizations must protect against cyberthreats throughout the entire customer journey—from first ad impression to visiting an application to navigating through an account to making a transaction.

Choosing a vendor that offers cybersecurity, fraud, and compliance solutions is crucial to implementing a defense-in-depth strategy as an organization scales. Furthermore, it facilitates collaboration and shared responsibility between security, compliance, and fraud teams.

Questions to ask about platform capabilities:

Does the vendor offer solutions that complement its bot mitigation capabilities?

Look for vendors that protect the customer journey across application, account and advertising surfaces. Key offerings include defense against fraud by fake accounts or compromised accounts, as well as tools to simplify PCI DSS 4 browser script compliance.

Does the solution take steps pre- and post-login to stop account takeover and fraud?

Look for a defense-in-depth solution that not only mitigates bots at login, but also serves as an early-warning system and identifies accounts that have been compromised post login.

Flagging logins with compromised credentials and forcing a password reset reduces the number of accounts that are vulnerable to takeover in the first place. On the other side of the account journey, detecting suspicious post-login behavior enables website owners to remediate breached accounts and minimize incidents of fraud.

Does the vendor have a leading threat intelligence team?

Augment industry-leading bot management technology with an industry-leading threat intelligence team that continuously investigates emerging threats and optimizes detection models accordingly. To determine threat intelligence expertise, look for providers that have published numerous high-profile investigations and disruptions of fraud schemes. This ensures that customers remain ahead of emerging threats and technological innovations, such as agentic AI.

Does the vendor have a track record of innovation in cybersecurity?

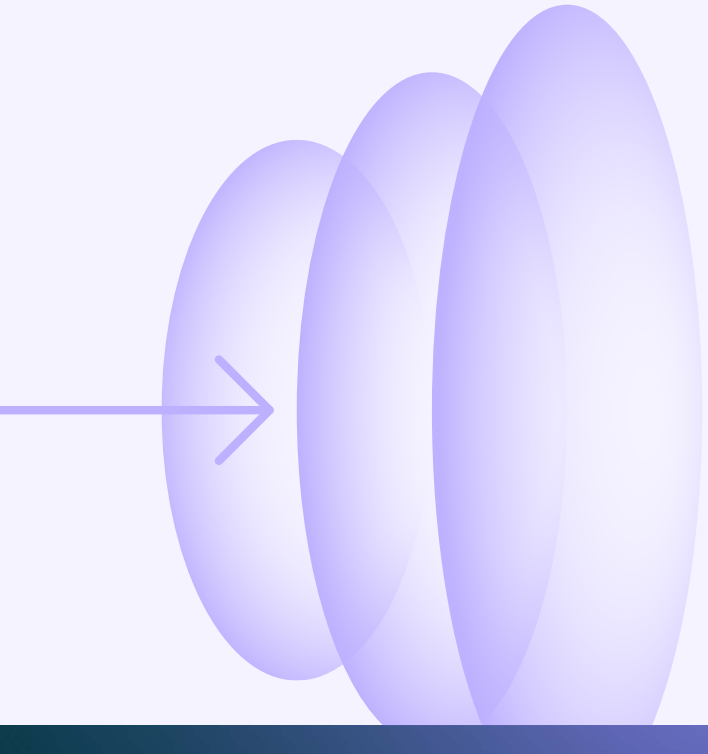
The cyberthreat landscape is always evolving, with bots growing increasingly sophisticated each day. Choosing a vendor on the cutting edge of innovation and product development vision for the future will ensure that even the most advanced attacks are mitigated with speed, scale, and decision precision.

Bot Management Specialist vs. CDN/ WAF Platform Add-On Solution

What about WAFs?

A web application firewall (WAF) is a security tool that filters and monitors HTTP/HTTPS traffic between a web application and the internet. It operates at the application layer and is specifically focused on detecting and blocking malicious traffic targeting web applications. WAFs use a variety of techniques to identify and mitigate threats, such as SQL injection, cross-site scripting (XSS), file inclusion, and other application-layer attacks.

When discussing a platform approach, organizations may default to web application and API protection (WAAP) solutions. WAAPs are critical and necessary for any cybersecurity security stack—but they are not sufficient alone for bot management. A new category of consolidated platforms has emerged, comprising specialist solutions that protect against bad bots and cyberfraud at every step of the customer journey.



When good enough isn't good enough

Specialist bot management solutions offer advanced detection, mitigation, and reporting capabilities to protect against sophisticated bots, which CDN and web application firewall (WAF) add-on tools often lack. Depending on your business needs, it might be necessary to opt for a specialist standalone solution or to add it as an extra layer of defense to the tool provided by your CDN/WAF vendor. Here are some questions to consider when making that choice:

Do you face evolving, sophisticated attackers?

Add-on solutions can sometimes be sufficient to mitigate common, one-and-done attacks. However, if your application is targeted by sophisticated adversaries, you will need a specialist solution that tracks and adapts to specific threats and optimizes response policies to ensure precise mitigation as attackers evolve their methods. Specialized detection, dedicated support and detailed dashboards enable investigation and analysis of advanced threats.

Do you have a mobile app? Is it native or hybrid?

CDN/WAF add-ons may not have a mobile SDK or may be limited in the types of mobile apps that they support. Without an SDK, bot management solutions must either allow all suspicious traffic tagged as mobile (potentially allowing fraudulent traffic through) or hard block all suspicious mobile traffic (increasing false positives). If you have a mobile app, it is critical for your bot management vendor to provide an easy-to-install mobile SDK that supports both native and hybrid apps. Even if the solution will be deployed first on your web app, it is important to consider the ease of adding mobile down the line.

Will you require custom ongoing management support?

Because they originate from your CDN/WAF vendor, add-on solutions are easier to spin up with fewer resources. However, unlike a CDN or WAF, bot management isn't set-it-and-forget-it. Using an add-on solution means that your team is responsible for managing the ongoing maintenance of rules and policies—or you may have to outsource it to a costly managed services team. Research potential vendors' customer support options and choose a solution that can be largely managed by your internal team.

Is a multi-vendor strategy the right approach?

In some cases, one might choose to deploy both an add-on and specialist solution. Many WAFs include anti-bot rulesets that, while definitely not a substitute for a dedicated bot management solution, could be part of a defense-in-depth strategy.

Are you monitoring fraud and abuse in customer accounts?

If online accounts are a key part of your business model, the ability to monitor them for fraud and abuse is key. In most cases this requires a specialized solution designed for that purpose. If using a CDN/WAF add-on, check that they are able to provide post-login monitoring, the capabilities outlined in this guide and automated mitigation to the standard required to reduce fraud.

Signal collection

In many cases, CDN/WAF vendors may only analyze edge traffic. This means that user activity data (such as mouse movements, keystrokes, and click patterns) is not analyzed. Such tools cannot match the detection accuracy of specialized solutions that also leverage a client-side sensor.

5.

HUMAN Security: A Bot Management Leader

HUMAN was named a Leader in The Forrester Wave™: Bot Management Software, Q3 2024. Our Application Protection package defends against malicious bots on web and mobile applications and APIs. The solution detects and mitigates automated attacks, including account takeover, scraping, transaction abuse, data contamination, and fake account creation. In addition, our secondary detection engine analyzes attack data post-decision to reveal previously unseen insights into individual attack characteristics and attacker actions, identify large-scale attack patterns, and continuously optimize mitigation flows.

HUMAN enables organizations to defend against automated manipulation, stop account fraud, and ensure a trusted application environment where users are safe to interact, log in, and transact. The Human Defense Platform looks beyond automated attacks to address cyberthreats throughout the end-to-end customer journey across advertising, application, and account surfaces.

Scale

We verify more than 20 trillion digital interactions weekly across 3 billion unique devices providing unrivaled threat telemetry.

Speed

Our decision engine examines 2,500-plus signals per interaction, connecting disparate data to detect anomalies in mere milliseconds.

Decision Precision

Signals from across the customer journey are analyzed by 400-plus algorithms and adaptive machine learning models to enable high-fidelity decisioning.

Don't Go It Alone

The bot management landscape is dynamic and complex. This buyers' guide provides a framework to help you determine the optimal solution for your business objectives and infrastructure environment.

Ultimately, success hinges on finding a bot management vendor that acts as a true partner. In the face of AI innovations, AI-controlled agents working alongside humans, and ever-evolving cyberattacks, visibility and agility are paramount. Your vendor must be able to provide full transparency, collaboration, and ongoing support to address emerging threats. Choose a trusted partner that will proactively anticipate your needs and help you stay ahead of the curve.

It Takes a Village to Buy Cybersecurity Software

Cyberfraud teams (including security and fraud analysts) are at the center of the bot management buying decision. However, there are many more stakeholders within your organization that need to be included—and even more who might typically not be involved, but who would benefit from such a solution. Look at the buying journey as an opportunity to engage different areas of your business to achieve a common security goal.

Potential departments to include:

COMPLIANCE

E-COMMERCE

AD OPERATIONS

FINANCE

GROWTH MARKETING

HUMAN

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit www.humansecurity.com.