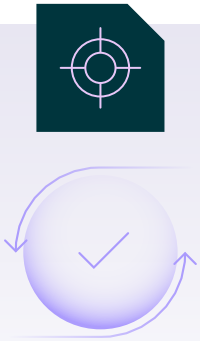
HUMAN

Bot Management Solution Buyers' Checklist

If you are purchasing a bot management technology, there are six key criteria that should shape your buying decision.

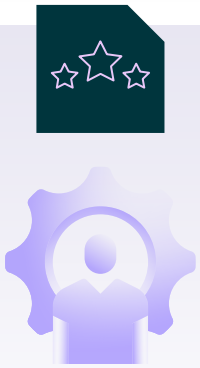
Whether you are buying your first bot management solution, a complementary solution, or replacing your current solution, it can be complex to evaluate numerous products and determine which one is right for your business.

This checklist outlines six criteria to consider, along with key questions to ask for each area. Buyers can discuss this criteria with the vendors themselves and conduct independent research using peer reviews and analyst reports, such as G2's seasonal grid and The Forrester Wave™: Bot Management Software, Q3 2024.



1. Efficacy

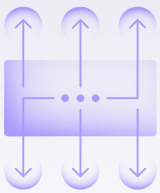
- How well does the solution defend against sophisticated attackers?
- Does the solution have secondary detection capabilities, such as the ability to profile attacks, automatically optimize mitigation flows, and respond to changing threats over time?
- Does the solution use advanced detection techniques and defense-in-depth strategies?



2. Impact on performance and user experience

- What is the latency impact? Are slow and expensive server-to-server (S2S) calls executed on every request without your control?
- What is the CAPTCHA experience like? How often are CAPTCHAs shown to human website visitors?
- Does the solution offer low-friction ways to verify humanity, such as pre-filtering malicious bots at the edge?

3. Ease of deployment and ongoing maintenance



- What resources will be required to deploy and manage this solution on an ongoing basis?
- Does the solution have a mobile SDK? Does it support hybrid apps and APIs in addition to web?
- How is the vendor's customer support?

4. AI agents and "good bot" management

- Does the solution provide visibility into known bots and AI agents over time?
- Can your organization customize responses to known bots and AI agents?
- Does the solution enable you to monetize AI bots and execute response actions depending on payment plan or other conditions?

5. Dashboards and reporting

- Does the customer console provide actionable attack-type dashboards and reports for different stakeholders?
- Does the solution surface insights from data analysis post-decision?
- Does the solution report on attacker profiles and characteristics to help jump-start and inform your investigations?

6. Platform capabilities

- Does the vendor offer solutions that complement its bot mitigation capabilities?
- Does the solution take steps pre- and post-login to stop account takeover and fraud?
- Does the vendor have a leading threat intelligence team and a track record of innovation in cybersecurity?

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.