



Bot and Fraud Management Checklist

Single-method security solutions are incomplete. Attackers blend bots, AI-driven deception, and human fraud to bypass security defenses. Defeating modern cyberthreats requires a comprehensive and extensible solution that combines layered detections, customizable mitigation, and guided investigative intelligence.

This checklist outlines seven 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 dedicated attackers?
- ☐ Can the solution identify human-led fraud and AI-traffic in addition to bots?
- ☐ 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? (E.g., pre, at and post-login account security)



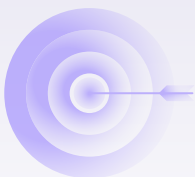
2. Impact on performance and app user experience



- ☐ 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?
- ☐ Does the solution offer low-friction ways to verify that the user of the account is legitimate? (E.g., sending an email to confirm)



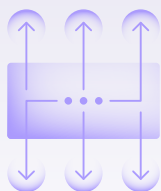
3. Ease of deployment and ongoing management



- ☐ 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?
- ☐ Does the solution collect personally identifiable information (PII)?
- ☐ How is the vendor's customer support?



4. Fraud monitoring and mitigation actions



- ☐ Can the solution monitor actions taken within an account and identify patterns of fraud?
- ☐ Is intelligence on compromised credentials offered?
- ☐ Does the solution offer custom mitigation actions? Can they integrate into your own systems such as CIAMs or SIEMs?
- ☐ Are API integrations available?



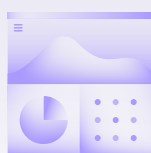
5. AI agents and "good bot" management



- ☐ 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?
- ☐ Does the solution protect against AI-generated cyberthreats?



6. 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 jumpstart and inform your investigations?
- ☐ Can you track your automatic mitigations without your team's involvement?



7. Platform capabilities



- ☐ Does the vendor offer solutions that complement its bot and fraud mitigation capabilities? (E.g., combatting ad fraud and malvertising)
- ☐ Does the vendor have a leading threat intelligence team?
- ☐ Does the vendor have a track record of innovation in cybersecurity?



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.