ABOUT

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**

RESOURCES

Human Defense for the Public Sector
carah.io/human-defense-brief

United States Federal Civilian Agency Simplifies Compliance to PCI DSS 4
carah.io/fed-civ-case-study

Defending Against Automated Threats Across Critical Systems Globally
carah.io/human-whitepaper

United States Federal Civilian Agency Stops Malvertising on Citizen-Facing Service
carah.io/malvertising-case-study

Mission-Critical Systems Under Attack: Defending Against GenAI-Bots

TECHNICAL SUMMARY

Generative AI (GenAI) bots are not just evolving—they are already on the attack. These autonomous cyber threats conduct reconnaissance, exploit security gaps faster than any human and modify attack patterns in real-time. Unlike traditional bots, GenAI can learn, adapt and outmaneuver static defenses. Combating such advanced threats requires an equally sophisticated defense that leverages automation to stay ahead. HUMAN Security rises to this challenge with over 400 AI- and machine learning (ML)-powered algorithms designed to detect, analyze and stop bots.

HUMAN Security takes a proactive approach, preventing bot-driven threats before they reach mission-critical systems. Unlike reactive security solutions, HUMAN integrates with Content Delivery Networks (CDNs) and over 200 systems via open Application Programming Interfaces (APIs) to intercept threats in real-time. This preemptive defense prevents credential stuffing attacks, fraudulent account creation and data scraping while maintaining a frictionless user experience. By blocking bots on the first request, HUMAN strengthens security for public sector systems without disrupting legitimate users.

THE CHALLENGE

For the public sector, bots are no longer just a cybersecurity nuisance—they have become a national security threat. Historically associated with ticket scalping or retail fraud, bots now target government systems, defense networks, taxpayer services and election infrastructure at machine speed. These attacks include credential stuffing—exemplified by the 2023 campaign targeting the U.S. Department of Education (Source: CISA)—where bots test stolen credentials to gain unauthorized access, as well as deepfake impersonations of government officials. With the ability to act as millions of users simultaneously, bots—often paired with AI-generated deepfakes—have been weaponized by hacking groups and nation-states to commit fraud, steal sensitive data and disrupt operations. In early 2024, for example, bad actors created a deepfake audio impersonation of a U.S. official that nearly led to the release of classified information (Source: Cybersecurity Information Sheet).

Traditional cybersecurity approaches struggle to keep pace with these evolving threats. GenAI bots do not follow static attack patterns; they learn adapt and modify their tactics mid-attack. Signature-based detections fail against these bots, which can mimic human behavior to bypass security measures such as the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAs). They hijack authenticated user sessions, exploit overlooked Zero Trust segments and repurpose compromised devices as Trojan horses to infiltrate networks. In late 2023, a foreign state-sponsored group bypassed multi-factor authentication (MFA) by leveraging AI-driven bots that swiftly probed for Zero Trust misconfigurations (Source: Mandiant).

Given these adaptive threats, bot mitigation must be powered by equally advanced, AI-driven defenses—positioning it as a core pillar of public sector cybersecurity alongside Zero Trust frameworks and real-time threat intelligence.

THE SOLUTION

HUMAN Security provides an advanced, AI-driven bot mitigation platform that detects and prevents bot-driven threats before they compromise mission-critical systems. By analyzing 20 trillion interactions weekly, across 4 billion devices, HUMAN applies over 400 AI and ML algorithms to detect anomalies and distinguish between legitimate users and bots with over 99% accuracy.

With experience protecting enterprises like Amazon, Google and Walmart—as well as federal entities like the U.S. Postal Service—HUMAN extends its expertise to public sector organizations, safeguarding against credential stuffing, identity fraud and deepfake bot attacks in real-time. This broad visibility allows HUMAN to detect and stop new botnet attacks (networks of compromised computers) before they escalate.

HUMAN's bot mitigation strategy is built on four key pillars:

1. **Early Detection** – Identifying bots before they reach critical systems.
2. **Behavioral Analysis** – Assessing intent beyond traffic patterns to distinguish harmless bots from malicious activity.
3. **Zero Trust Integration** – Addressing the Zero Trust bot gap, where bots exploit unprotected environments to compromise government workers' devices.
4. **Automated Response** – Providing collective protection, where an attack against one organization strengthens defenses across the network.

Rather than relying on traditional CAPTCHA methods, HUMAN employs behavioral AI to deliver a seamless user experience. The AI continuously analyzes activity in real-time, assigning a risk score from 0 to 100 to determine whether to allow or block access. This ensures legitimate users can proceed without disruption while effectively stopping malicious bots. Designed to minimize false positives, HUMAN's security operates invisibly, safeguarding critical systems without interfering with user access.

Effective security relies on context. HUMAN's approach goes beyond isolated actions, analyzing 2,500 behavioral signals to distinguish between humans and bots with precision. By continuously refining its ML models, HUMAN adapts in real-time, detecting subtle anomalies such as changes in typing speed or navigation patterns. With over a decade of experience, HUMAN has built an extensive device history, allowing it to recognize when a previously legitimate device begins exhibiting suspicious behavior. By focusing on the most relevant threats, HUMAN ensures security teams can prioritize real risks while avoiding unnecessary disruptions.

CONTACT US HUMANSecurity@carahsoft.com • 844-214-4790 • www.carahsoft.com/human-security

HUMAN | carahsoft.