HUMAN

Agentic AI: Transforming Citizen Services in the Public Sector

Artificial Intelligence (AI) is transforming how citizens interact with government agencies, making essential public services more efficient, accessible, and responsive. One of the most exciting developments is Agentic AI—AI that operates with a level of autonomy, making decisions, taking proactive actions, and adapting over time.

While Agentic AI has the potential to drastically improve public sector services, it also introduces significant risks that must be addressed to protect citizens and government operations.

The benefits of agentic AI in citizen services

Agentic AI goes beyond traditional AI chatbots by anticipating needs and taking actions on behalf of citizens. Here are some examples of how Agentic AI can reshape public sector services:

Proactive service delivery

Agentic AI can automate and enhance citizen interactions, such as helping a taxpayer file a return, flagging errors, and recommending deductions. At the Social Security Administration (SSA), Agentic AI can manage ongoing claims and proactively update beneficiaries, improving both citizen satisfaction and operational efficiency.

Personalized assistance across channels

By bridging multiple service channels—online portals, emails, and phone calls—Agentic AI offers a personalized experience. For veterans, an AI system could assist with navigating healthcare benefits and scheduling appointments based on their needs, continually learning and adjusting to deliver better support.

Reducing processing times and human error

AI can automate routine tasks in complex processes, reducing human error and speeding up service delivery. The IRS, for instance, could automate tax filing assistance, improving both accuracy and speed, while freeing up human agents for more complex issues.

AI-driven decision-making for public assistance

In programs like unemployment benefits, Agentic AI can autonomously analyze personal data to assess eligibility and flag inconsistencies, speeding up processing and reducing backlogs. This helps streamline applications and reduces delays in critical public assistance.

The risks of agentic AI in the public sector

While the benefits are clear, the integration of Agentic AI also comes with risks that must be carefully managed:

Unintended consequences of AI site integrations

Many government websites use AI-driven systems like chatbots to assist citizens. These integrations can improve efficiency but also introduce the risk of AI making decisions or providing information that doesn't align with user intent. A notable example is a Canadian court case where a customer was awarded damages after receiving incorrect advice from a chatbot. Public agencies must ensure that these systems are accountable and transparent to avoid such issues.

PII and data privacy risks

Citizen services handle vast amounts of personally identifiable information (PII), such as tax details or healthcare records. The use of Agentic AI to collect and process this data raises concerns about data privacy. A breach or misuse of this information could lead to identity theft or unauthorized access to sensitive data, particularly in services that handle vulnerable populations.

Potential misuse for DDoS and automated attacks

As AI technologies become more accessible, they lower the barrier for malicious actors, including hacktivists and cybercriminals, to orchestrate large-scale attacks. AI-driven Distributed Denial of Service (DDoS) attacks, for example, could overwhelm public sector websites, causing service outages and eroding public trust. Hackers also potentially leverage AI to amplify attacks, making government platforms prime targets for cybercrime.

Protecting public sector services with HUMAN Security

HUMAN Security provides best-in-class bot mitigation capabilities. With our unparalleled visibility into 20 trillion interactions each week, we can detect all forms of automation, including sophisticated bots and bot-controlled browsers—whether or not they are powered by AI. When bots are detected, a "press-and-hold" challenge is served, ensuring that you always keep a "human-in-the-loop."

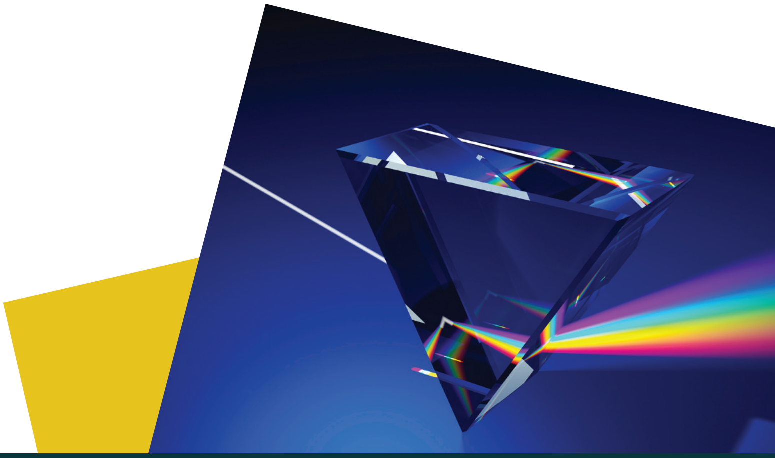
Using HUMAN's platform, our customers also have access to the best-in-class management of known bots and crawlers.

To unlock the full potential of Agentic AI while minimizing its risks, public sector organizations can turn to HUMAN Security for advanced protection. Here's how HUMAN Security can help:

- **Bot Detection and Prevention:** HUMAN Security's AI-driven bot detection technology can prevent malicious bots from exploiting vulnerabilities in public sector websites, ensuring that only legitimate users interact with services. This helps mitigate the risk of DDoS and other automated cyberattacks.
- **Fraud Detection and Prevention:** HUMAN's advanced fraud detection systems can help identify and stop AI-driven fraud before it impacts citizens or government services. This technology is crucial for protecting PII and ensuring compliance with privacy regulations.

By implementing HUMAN Security's solutions, public sector agencies can harness the power of Agentic AI without exposing themselves to significant security risks. HUMAN Security ensures that these innovative technologies remain safe, secure, and trustworthy, ultimately enhancing the citizen experience and protecting sensitive data.

Learn more about how we provide mission-critical end-to-end protection for the public sector at www.humansecurity.com/platform/industry/public-sector.



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**