Wikipedia
The Free Encyclopedia

Agentic AI

In the context of generative artificial intelligence, **AI agents** (also referred to as **compound AI systems** or **agentic AI**) are a class of intelligent agents distinguished by their ability to operate autonomously in complex environments. Agentic AI tools prioritize decision-making over content creation and do not require human prompts or continuous oversight.[1]

Overview

AI agents possess several key attributes, including complex goal structures, natural language interfaces, the capacity to act independently of user supervision, and the integration of software tools or planning systems. Their control flow is frequently driven by large language models (LLMs).[2] Agents also include memory systems for remembering previous user-agent interactions and orchestration software for organizing agent components.[3]

Researchers and commentators have noted that AI agents do not have a standard definition.[2][4][5][6] The concept of agentic AI has been compared to the fictional character J.A.R.V.I.S..[7]

A common application of AI agents is the automation of tasks—for example, booking travel plans based on a user's prompted request.[8][9] Prominent examples include Devin AI, AutoGPT, and SIMA.[10] Further examples of agents released since 2025 include OpenAI Operator,[11] ChatGPT Deep Research,[12] Manus,[13] Quark (based on Qwen),[14] AutoGLM Rumination,[14] and Coze (by ByteDance).[14] Frameworks for building AI agents include LangChain,[15] as well as tools such as CAMEL,[16][17] Microsoft AutoGen,[18] and OpenAI Swarm.[19]

Companies such as Google, Microsoft and Amazon Web Services have offered platforms for deploying pre-built AI agents.[20]

Proposed protocols for standardizing inter-agent communication include the Agent Protocol (by LangChain), the Model Context Protocol (by Anthropic), AGNTCY,[21] Gibberlink,[22] the Internet of Agents,[23] Agent2Agent (by Google),[24] and the Agent Network Protocol.[25] Some of these protocols are also used for connecting agents with external applications.[3] Software frameworks for addressing agent reliability include AgentSpec, ToolEmu, GuardAgent, Agentic Evaluations, and predictive models from H2O.ai.[26]

In February 2025, Hugging Face released Open Deep Research, an open source version of OpenAI Deep Research.[27] Hugging Face also released a free web browser agent, similar to OpenAI Operator.[28] Galileo AI published on Hugging Face a leadership board for agents, which ranks their performance based on their underlying LLMs.[29]

Memory systems for agents include Mem0,[30][31] MemGPT,[32] and MemOS.[33]

History

AI agents have been traced back to research from the 1990s, with Harvard professor Milind Tambe noting that the definition of an AI agent was not clear at the time either. Researcher Andrew Ng has been credited with spreading the term "agentic" to a wider audience in 2024.[34]

Training and testing

Researchers have attempted to build world models[35][36] and reinforcement learning environments[37] to train or evaluate AI agents. For example, video games such as Minecraft[38] and No Man's Sky[39] as well as replicas of company websites,[40] have also been used for training AI agents.

Autonomous capabilities

The *Financial Times* compared the autonomy of AI agents to the SAE classification of self-driving cars, comparing most applications to level 2 or level 3, with some achieving level 4 in highly specialized circumstances, and level 5 being theoretical.[41]

Architectural patterns

Common architectural design patterns for agents include:

- Retrieval-augmented generation[42]
- ReAct (Reason + Act),[43] an extension of chain-of-thought prompting that queries the underlying model to explain its reasoning before taking any action.[44]
- Reflexion,[42][43][44] which uses an LLM to create feedback on the agent's plan of action and stores that feedback in a memory cache.
- A tool/agent registry,[42] for organizing software functions or other agents that the agent can use.
- One-shot model querying,[42] which queries the model once to create the plan of action.

Multimodal AI agents

In addition to large language models (LLMs), vision-language models (VLMs) and multimodal foundation models can be used as the basis for agents. In September 2024, Allen Institute for AI released an open-source vision-language model, which *Wired* noted could give AI agents the ability to perform complex computer tasks, including the possibility of automated computer hacking.[45] Nvidia released a framework for developers to use VLMs, LLMs and retrieval-augmented generation for building AI agents that can analyze images and videos, including video search and video summarization.[46][47] Microsoft released a multimodal agent model – trained on images, video, software user interface interactions, and robotics data – that the company claimed can manipulate software and robots.[48]

Applications

As of April 2025, per the Associated Press, there are few real-world applications of AI agents.[49] As of June 2025, per *Fortune*, many companies are primarily experimenting with AI agents.[50]

A recruiter for the Department of Government Efficiency proposed in April 2025 to use AI agents to automate the work of about 70,000 United States federal government employees, as part of a startup with funding from OpenAI and a partnership agreement with Palantir. This proposal was criticized by experts for its impracticality, if not impossibility, and the lack of corresponding widespread adoption by businesses.[51]

The Information divided AI agents into seven archetypes: business-task agents, for acting within enterprise software; conversational agents, which act as chatbots for customer support; research agents, for querying and analyzing information (such as OpenAI Deep Research); analytics agents, for analyzing data to create reports; software developer or coding agents (such as Cursor); domain-specific agents, which include specific subject matter knowledge; and web browser agents (such as OpenAI Operator).[3]

By mid-2025, AI agents have been used in video game development,[52] gambling (including sports betting),[53] and cryptocurrency wallets[53] (including cryptocurrency trading and meme coins[54]). In August 2025, *New York Magazine* described software development as the most definitive use case of AI agents.[55] Likewise, by October 2025, noting a decline in expectations, *The Information* noted AI coding agents and customer support as the primary use cases by businesses.[56]

AI agents have also been integrated into operating systems. Writing in *The Economist*, Signal president Meredith Whittaker has noted that agents have been included in operating systems developed by Microsoft, Apple and Google.[57] In November 2025, Microsoft released a test software build of Windows 11 that included agents intended to run background tasks, with the ability to read and write personal files.[58] In December 2025, ByteDance released Doubao, an AI agent that can be integrated into smartphone operating systems, particularly the Nubia M153 by ZTE.[59] Several apps in China blocked or restricted the agent, citing privacy and security concerns,[60] including WeChat,[59] Alipay, Taobao, Pinduoduo, Ele.me,[61] and local banks.[62]

In November 2025, *The Wall Street Journal* reported that few companies that deployed AI agents have received a return on investment.[63]

Several government bodies in the United States and United Kingdom have deployed or announced the deployment of agents. The city of Kyle, Texas deployed an AI agent from Salesforce in March 2025 for 311 customer service.[64] In November 2025, the Internal Revenue Service stated that it would use Agentforce, AI agents from Salesforce, for the Office of Chief Counsel, Taxpayer Advocate Services and the Office of Appeals.[65] That same month, Staffordshire Police announced that they would trial Agentforce agents for handling non-emergency 101 calls in the United Kingdom starting in 2026.[66] In December 2025, the Food and Drug Administration announced that it would offer "agentic AI capabilities" to its staff for "meeting management, pre-market reviews, review validation, post-market surveillance, inspections and compliance and administrative functions."[67] That same month, the United States Department of Defense launched GenAI.mil, an internal platform for American military personnel to use generative AI-based applications based on Google Gemini, including "intelligent agentic workflows". Defense Secretary Pete Hegseth listed applications such as "[conducting] deep research, [formatting] documents and even [analyzing] video or imagery at unprecedented speed."[68]

Web browsing

Web browsers with integrated AI agents are sometimes called agentic browsers. Such agents can perform small tedious tasks during web browsing and potentially even perform browser actions on behalf of the user. Products like OpenAI Operator and Perplexity Comet integrate a spectrum of AI capabilities including the ability to browse the web, interact with websites and perform actions on behalf of the user.[69][70] In 2025, Microsoft launched NLWeb, an agentic web search replacement that would allow websites to use agents to query content from websites by using RSS-like interfaces that allow for the lookup and semantic retrieval of content.[71] Products integrating agentic web capabilities have been criticised for exfiltrating information about their users to third-party servers[72] and exposing security issues since the way the agents communicate often occur through non-standard protocols.[71]

Proposed benefits

Proponents argue that AI agents can increase personal and economic productivity,[9][73] foster greater innovation,[74] and liberate users from monotonous tasks.[74][75] A *Bloomberg* opinion piece by Parmy Olson argued that agents are best suited for narrow, repetitive tasks with low risk.[76] Conversely, researchers suggest that agents could be applied to web accessibility for people who have disabilities,[77][78] and researchers at Hugging Face propose that agents could be used for coordinating resources such as during disaster response.[79] The R&D Advisory Team of the BBC views AI agents as being most useful when their assigned goal is uncertain.[80] Erik Brynjolfsson suggests that AI agents are more valuable enhancing, rather than replacing, humans.[81]

Concerns

Concerns include potential issues of liability,[73][80] an increased risk of cybercrime,[8][73] ethical challenges,[73] as well as problems related to AI safety[73] and AI alignment.[8][75] Other issues involve data privacy,[8][82] weakened human oversight,[8][73][79] a lack of guaranteed repeatability,[83] reward hacking,[84] algorithmic bias,[82][85] compounding software errors,[8][10] lack of explainability of agents' decisions,[8][86] security vulnerabilities,[8][87] stifling competition,[57] problems with underemployment,[85] job displacement,[9][85] cognitive offloading,[88] and the potential for user manipulation,[86][89] misinformation[79] or malinformation.[79] They may also complicate legal frameworks and risk assessments, foster hallucinations, hinder countermeasures against rogue agents, and suffer from the lack of standardized evaluation methods.[90][8][91] They have also been criticized for being expensive[2][8] and having a negative impact on internet traffic,[8] and potentially on the environment due to high energy usage.[83][92][93] According to an estimation by Nvidia CEO Jensen Huang, AI agents would require 100 times more computing power than LLMs.[94] There is also the risk of increased concentration of power by political leaders, as AI agents may not question instructions in the same way that humans would.[84]

Journalists have described AI agents as part of a push by Big Tech companies to "automate everything".[95] Several CEOs of those companies have stated in early 2025 that they expect AI agents to eventually "join the workforce".[96][97] However, in a preprint study, Carnegie Mellon University researchers tested the behavior of agents in a simulated software company and found that none of the agents could complete a majority of the assigned tasks.[96][98] Other researchers had similar findings with Devin AI[99] and other agents in business settings[100][101] and freelance work.[102] *CNN* argued that statements by CEOs on the potential replacement of their employees by AI agents were a strategy to "[keep] workers working by making them afraid of losing their jobs."[103] Tech companies have pressured employees to use generative AI models in their work, including AI coding agents. Brian Armstrong, the CEO of Coinbase, fired several employees who did not.[104][105] Some business leaders have replaced some of their employees with agents, but have said that the agents would need more supervision than those employees.[56] *Futurism* questioned whether Amazon's previously announced efforts to replace parts of its workforce with generative AI and AI agents could have led to the October 2025 outage of Amazon Web Services.[106]

Yoshua Bengio warned at the 2025 World Economic Forum that "all of the catastrophic scenarios with AGI or superintelligence happen if we have agents".[107]

In March 2025, Scale AI signed a contract with the United States Department of Defense to work with them, in collaboration with Anduril Industries and Microsoft, to develop and deploy AI agents for the purpose of assisting the military with "operational decision-making".[108] In July 2025, Fox Business reported that the company EdgeRunner AI built an offline agent, compressed and fine-tuned on military information, with the CEO seeing more common LLMs as "heavily politicized to the left". As of that time, the company model is being used by the United States Special Operations Command in an overseas deployment.[109] Researchers have expressed concerns that agents and the large language models they are based on could be biased towards aggressive foreign policy decisions.[110][111]

Research-focused agents have the risk of consensus bias and coverage bias due to collecting information available on the public Internet.[112] *NY Mag* unfavorably compared the user workflow of agent-based web browsers to Amazon Alexa, which was "software talking to software, not humans talking to software pretending to be humans to use software."[113] The same outlet described web browser agents and computer-use agents as an attempt to "click-farm the entire economy."[114]

Agents have been linked to the dead Internet theory due to their ability to both publish and engage with online content.[115]

Agents may get stuck in infinite loops.[11][116]

Since many inter-agent protocols are being developed by large technology companies, there are concerns that those companies could use these protocols for self-benefit.[25]

A June 2025 Gartner report accused many projects described as agentic AI of being rebrands of previously released products, terming the phenomenon as "agent washing".[55]

Researchers have warned about the impact of providing AI agents access to cryptocurrency and smart contracts.[54]

During a vibe coding experiment, a coding agent by Replit deleted a production database during a code freeze, "[covered] up bugs and issues by creating fake data [and] fake reports" and responded with false information.[117][118] A user of Google Antigravity reported that, when the user attempted to use the system to delete cache, the system responded by deleting the user's D hard drive.[119]

In July 2025, PauseAI referred OpenAI to the Australian Federal Police, accusing the company of violating Australian laws through ChatGPT agent due to the risk of assisting the development of biological weapons.[120]

Issues with multi-agent systems include few coordination protocols between component agents, inconsistent performance, and challenges debugging.[121]

In November 2025, Anthropic claimed that a group of hackers sponsored by China attempted a cyberattack against at least 30 organizations by using Claude Code in an agentic workflow, and that several of these infiltrations had succeeded.[122] However, independent cybersecurity researchers questioned the significance of Anthropic's findings.[122][123]

Whittaker argued that the push by Big Tech companies to deploy AI agents risked security vulnerabilities across the Internet.[124]

Possible mitigation

Zico Kolter noted the possibility of emergent behavior as a result of interactions between agents, and proposed research in game theory to model the risks of these interactions.[125]

Guardrails, defined by *Business Insider* as "filters, rules, and tools that can be used to identify and remove inaccurate content" have been suggested to help reduce errors.[126]

To address security vulnerabilities related to data access, language models could be redesigned to separate instructions and data, or agentic applications could be required to include guardrails. These ideas were proposed in response to a zero-click exploit that affected Microsoft 365 Copilot.[50] Confidential computing has been proposed for protecting data security in projects involving AI agents and generative AI.[127]

A pre-print by Nvidia researchers has suggested small language models (SLMs) as an alternative to LLMs for AI agents, arguing that SLMs are cheaper and more energy efficient.[128][129]

The Economist has advised avoiding what Simon Willison has described as the "lethal trifecta" for AI agents and LLMs: "outside-content exposure, private-data access and outside-world communication".[130]

See also

- Intelligent agent
- Model Context Protocol
- Rational agent
- Robotic process automation
- Software agent

References

1. Purdy, Mark (December 12, 2024). "What Is Agentic AI, and How Will It Change Work?" (https://hbr.org/2024/12/what-is-agentic-ai-and-how-will-it-change-work). *Harvard Business Review*. ISSN 0017-8012 (https://search.worldcat.org/issn/0017-8012). Retrieved April 24, 2025.
2. Kapoor, Sayash; Stroebl, Benedikt; Siegel, Zachary S.; Nadgir, Nitya; Narayanan, Arvind (2024). "AI Agents That Matter". arXiv:2407.01502 (https://arxiv.org/abs/2407.01502) [cs.LG (https://arxiv.org/archive/cs.LG)].
3. Holmes, Aaron (July 7, 2025). "The Seven Kinds of AI Agents" (https://archive.today/20250720144318/https://www.theinformation.com/articles/seven-kinds-ai-agents). *The Information*. Archived from the original (https://www.theinformation.com/articles/seven-kinds-ai-agents) on July 20, 2025. Retrieved November 9, 2025.
4. Zeff, Maxwell; Wiggers, Kyle (March 14, 2025). "No one knows what the hell an AI agent is" (https://web.archive.org/web/20250318134231/https://techcrunch.com/2025/03/14/no-one-knows-what-the-hell-an-ai-agent-is/). *TechCrunch*. Archived from the original (https://techcrunch.com/2025/03/14/no-one-knows-what-the-hell-an-ai-agent-is/) on March 18, 2025. Retrieved May 15, 2025.
5. Varanasi, Lakshmi. "AI agents are all the rage. But no one can agree on what they do" (https://web.archive.org/web/20250411143511/https://www.businessinsider.com/what-is-an-ai-agent-depends-who-you-ask-2025-3). *Business Insider*. Archived from the original (https://www.businessinsider.com/what-is-an-ai-agent-depends-who-you-ask-2025-3) on April 11, 2025. Retrieved May 15, 2025.
6. Bort, Julie (May 12, 2025). "Even a16z VCs say no one really knows what an AI agent is" (https://web.archive.org/web/20250512184704/https://techcrunch.com/2025/05/12/even-a16z-vcs-say-no-one-really-knows-what-an-ai-agent-is/). *TechCrunch*. Archived from the original (https://techcrunch.com/2025/05/12/even-a16z-vcs-say-no-one-really-knows-what-an-ai-agent-is/) on May 12, 2025. Retrieved May 15, 2025.
7. Field, Hayden (August 31, 2025). "AI agents are science fiction not yet ready for primetime" (https://web.archive.org/web/20250915055451/https://www.theverge.com/the-stepback-newsletter/767376/ai-agents-jarvis-what-can-they-do). *The Verge*. Archived from the original (https://www.theverge.com/the-stepback-newsletter/767376/ai-agents-jarvis-what-can-they-do) on September 15, 2025. Retrieved November 9, 2025.
8. "AI Agents: The Next Generation of Artificial Intelligence" (https://web.archive.org/web/20250111192703/https://natlawreview.com/article/next-generation-ai-here-come-agents). *The National Law Review*. December 30, 2024. Archived from the original (https://natlawreview.com/article/next-generation-ai-here-come-agents) on January 11, 2025. Retrieved January 14, 2025.
9. "What are the risks and benefits of 'AI agents'?" (https://web.archive.org/web/20241228013835/https://www.weforum.org/stories/2024/12/ai-agents-risks-artificial-intelligence/). *World Economic Forum*. December 16, 2024. Archived from the original (https://www.weforum.org/stories/2024/12/ai-agents-risks-artificial-intelligence/) on December 28, 2024. Retrieved January 14, 2025.
10. Knight, Will (March 14, 2024). "Forget Chatbots. AI Agents Are the Future" (https://web.archive.org/web/20250105095231/https://www.wired.com/story/fast-forward-forget-chatbots-ai-agents-are-the-future/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/fast-forward-forget-chatbots-ai-agents-are-the-future/) on January 5, 2025. Retrieved January 14, 2025.

11. Marshall, Matt (February 22, 2025). "The rise of browser-use agents: Why Convergence's Proxy is beating OpenAI's Operator" (https://web.archive.org/web/20250222231546/https://venturebeat.com/ai/the-rise-of-browser-use-agents-why-convergences-proxy-is-beating-openais-operator/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/the-rise-of-browser-use-agents-why-convergences-proxy-is-beating-openais-operator/) on February 22, 2025. Retrieved April 2, 2025.
12. Milmo, Dan (February 3, 2025). "OpenAI launches 'deep research' tool that it says can match research analyst" (https://web.archive.org/web/20250203142402/https://www.theguardian.com/technology/2025/feb/03/openai-deep-research-agent-chatgpt-deepseek). *The Guardian*. ISSN 0261-3077 (https://search.worldcat.org/issn/0261-3077). Archived from the original (https://www.theguardian.com/technology/2025/feb/03/openai-deep-research-agent-chatgpt-deepseek) on February 3, 2025. Retrieved April 2, 2025.
13. Chen, Caiwei (March 11, 2025). "Everyone in AI is talking about Manus. We put it to the test" (https://web.archive.org/web/20250312113852/https://www.technologyreview.com/2025/03/11/1113133/manus-ai-review/). *MIT Technology Review*. Archived from the original (https://www.technologyreview.com/2025/03/11/1113133/manus-ai-review/) on March 12, 2025. Retrieved April 2, 2025.
14. "China is gaining ground in the global race to develop AI agents" (https://web.archive.org/web/20250602111847/https://restofworld.org/2025/china-ai-agent-openai/). *Rest of World*. June 2, 2025. Archived from the original (https://restofworld.org/2025/china-ai-agent-openai/) on June 2, 2025. Retrieved June 12, 2025.
15. David, Emilia (December 30, 2024). "Why 2025 will be the year of AI orchestration" (https://web.archive.org/web/20241230175615/https://venturebeat.com/ai/three-ways-2025-will-be-the-year-of-agentic-productivity/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/three-ways-2025-will-be-the-year-of-agentic-productivity/) on December 30, 2024. Retrieved January 14, 2025.
16. "CAMEL: Finding the Scaling Law of Agents. The first and the best multi-agent framework" (https://github.com/camel-ai/camel/). *GitHub*.
17. Li, Guohao (2023). "Camel: Communicative agents for "mind" exploration of large language model society" (https://proceedings.neurips.cc/paper_files/paper/2023/file/a3621ee907def47c1b952ade25c67698-Paper-Conference.pdf) (PDF). *Advances in Neural Information Processing Systems*. **36**: 51991–52008. arXiv:2303.17760 (https://arxiv.org/abs/2303.17760). S2CID 257900712 (https://api.semanticscholar.org/CorpusID:257900712).
18. Dickson, Ben (October 3, 2023). "Microsoft's AutoGen framework allows multiple AI agents to talk to each other and complete your tasks" (https://web.archive.org/web/20241227061127/https://venturebeat.com/ai/microsofts-autogen-framework-allows-multiple-ai-agents-to-talk-to-each-other-and-complete-your-tasks/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/microsofts-autogen-framework-allows-multiple-ai-agents-to-talk-to-each-other-and-complete-your-tasks/) on December 27, 2024. Retrieved January 14, 2025.
19. "The next AI wave — agents — should come with warning labels" (https://web.archive.org/web/20250114023632/https://www.computerworld.com/article/3727412/the-next-ai-wave-agents-should-come-with-warning-labels.html). *Computerworld*. January 13, 2025. Archived from the original (https://www.computerworld.com/article/3727412/the-next-ai-wave-agents-should-come-with-warning-labels.html) on January 14, 2025. Retrieved January 14, 2025.
20. David, Emilia (April 15, 2025). "Moveworks joins AI agent library craze" (https://web.archive.org/web/20250415214729/https://venturebeat.com/ai/moveworks-joins-ai-agent-library-craze/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/moveworks-joins-ai-agent-library-craze/) on April 15, 2025. Retrieved May 14, 2025.

21. David, Emilia (March 6, 2025). "A standard, open framework for building AI agents is coming from Cisco, LangChain and Galileo" (https://web.archive.org/web/20250309045209/https://venturebeat.com/ai/a-standard-open-framework-for-building-ai-agents-is-coming-from-cisco-langchain-and-galileo/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/a-standard-open-framework-for-building-ai-agents-is-coming-from-cisco-langchain-and-galileo/) on March 9, 2025. Retrieved April 2, 2025.
22. Zeff, Maxwell (March 5, 2025). "GibberLink lets AI agents call each other in robo-language" (https://web.archive.org/web/20250305141006/https://techcrunch.com/2025/03/05/gibberlink-lets-ai-agents-call-each-other-in-robo-language/). *TechCrunch*. Archived from the original (https://techcrunch.com/2025/03/05/gibberlink-lets-ai-agents-call-each-other-in-robo-language/) on March 5, 2025. Retrieved April 2, 2025.
23. Cooney, Michael (January 30, 2025). "Cisco touts 'Internet of Agents' for secure AI agent collaboration" (https://web.archive.org/web/20250131133538/https://www.networkworld.com/article/3812618/cisco-touts-internet-of-agents-for-secure-ai-agent-collaboration.html). *Network World*. Archived from the original (https://www.networkworld.com/article/3812618/cisco-touts-internet-of-agents-for-secure-ai-agent-collaboration.html) on January 31, 2025. Retrieved April 2, 2025.
24. Clark, Lindsay (April 10, 2025). "Did someone say AI agents, Google asks, bursting in" (https://web.archive.org/web/20250410112802/https://www.theregister.com/2025/04/10/google_agentic_ai_cloud_next/). *The Register*. Archived from the original (https://www.theregister.com/2025/04/10/google_agentic_ai_cloud_next/) on April 10, 2025. Retrieved May 14, 2025.
25. Stokel-Walker, Chris (June 11, 2025). "Can we stop big tech from controlling the internet with AI agents?" (https://archive.today/20250611131453/https://www.newscientist.com/article/2483880-can-we-stop-big-tech-from-controlling-the-internet-with-ai-agents/). *New Scientist*. Archived from the original (https://www.newscientist.com/article/2483880-can-we-stop-big-tech-from-controlling-the-internet-with-ai-agents/) on June 11, 2025. Retrieved June 12, 2025.
26. David, Emilia (March 28, 2025). "New approach to agent reliability, AgentSpec, forces agents to follow rules" (https://web.archive.org/web/20250412120324/https://venturebeat.com/ai/new-approach-to-agent-reliability-agentspec-forces-agents-to-follow-rules/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/new-approach-to-agent-reliability-agentspec-forces-agents-to-follow-rules/) on April 12, 2025. Retrieved May 14, 2025.
27. Edwards, Benj (February 5, 2025). "Hugging Face clones OpenAI's Deep Research in 24 hours" (https://web.archive.org/web/20250206125754/https://arstechnica.com/ai/2025/02/after-24-hour-hackathon-hugging-faces-ai-research-agent-nearly-matches-openais-solution/). *Ars Technica*. Archived from the original (https://arstechnica.com/ai/2025/02/after-24-hour-hackathon-hugging-faces-ai-research-agent-nearly-matches-openais-solution/) on February 6, 2025. Retrieved April 2, 2025.
28. Wiggers, Kyle (May 6, 2025). "Hugging Face releases a free Operator-like agentic AI tool" (https://web.archive.org/web/20250506221518/https://techcrunch.com/2025/05/06/hugging-face-releases-a-free-operator-like-agentic-ai-tool/). *TechCrunch*. Archived from the original (https://techcrunch.com/2025/05/06/hugging-face-releases-a-free-operator-like-agentic-ai-tool/) on May 6, 2025. Retrieved May 14, 2025.
29. Ortiz, Sabrina (February 14, 2025). "Which AI agent is the best? This new leaderboard can tell you" (https://web.archive.org/web/20250330001709/https://www.zdnet.com/article/which-ai-agent-is-the-best-this-new-leaderboard-can-tell-you/). *ZDNET*. Archived from the original (https://www.zdnet.com/article/which-ai-agent-is-the-best-this-new-leaderboard-can-tell-you/) on March 30, 2025. Retrieved April 2, 2025.

30. Dickson, Ben (May 8, 2025). "Mem0's scalable memory promises more reliable AI agents that remembers context across lengthy conversations" (http://web.archive.org/web/20250827005641/https://venturebeat.com/ai/mem0s-scalable-memory-promises-more-reliable-ai-agents-that-remembers-context-across-lengthy-conversations/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/mem0s-scalable-memory-promises-more-reliable-ai-agents-that-remembers-context-across-lengthy-conversations/) on August 27, 2025. Retrieved November 28, 2025.
31. Kene-Okafor, Tage (October 28, 2025). "Mem0 raises $24M from YC, Peak XV and Basis Set to build the memory layer for AI apps" (https://archive.ph/0G5cH). *TechCrunch*. Archived from the original (https://techcrunch.com/2025/10/28/mem0-raises-24m-from-yc-peak-xv-and-basis-set-to-build-the-memory-layer-for-ai-apps/) on October 28, 2025. Retrieved November 28, 2025.
32. Bort, Julie (September 23, 2024). "Letta, one of UC Berkeley's most anticipated AI startups, has just come out of stealth" (https://web.archive.org/web/20251006164502/https://techcrunch.com/2024/09/23/letta-one-of-uc-berkeleys-most-anticipated-ai-startups-has-just-come-out-of-stealth/). *TechCrunch*. Archived from the original (https://techcrunch.com/2024/09/23/letta-one-of-uc-berkeleys-most-anticipated-ai-startups-has-just-come-out-of-stealth/) on October 6, 2025. Retrieved November 28, 2025.
33. Nuñez, Michael (July 8, 2025). "Chinese researchers unveil MemOS, the first 'memory operating system' that gives AI human-like recall" (http://web.archive.org/web/20250901004623/https://venturebeat.com/ai/chinese-researchers-unveil-memos-the-first-memory-operating-system-that-gives-ai-human-like-recall/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/chinese-researchers-unveil-memos-the-first-memory-operating-system-that-gives-ai-human-like-recall/) on September 1, 2025. Retrieved November 28, 2025.
34. O'Brien, Matt (November 18, 2025). "What does 'agentic' AI mean? Tech's newest buzzword is a mix of marketing fluff and real promise" (https://web.archive.org/web/20251118171507/https://apnews.com/article/agentic-ai-agents-microsoft-amazon-518d6ae159d1f4d3343e98a456cb5221). *Associated Press*. Archived from the original (https://apnews.com/article/agentic-ai-agents-microsoft-amazon-518d6ae159d1f4d3343e98a456cb5221) on November 18, 2025. Retrieved November 28, 2025.
35. Knight, Will (May 22, 2025). "A United Arab Emirates Lab Announces Frontier AI Projects—and a New Outpost in Silicon Valley" (https://web.archive.org/web/20250522202354/https://www.wired.com/story/the-united-arab-emirates-announces-frontier-ai-projects-and-a-new-lab-in-silicon-valley/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/the-united-arab-emirates-announces-frontier-ai-projects-and-a-new-lab-in-silicon-valley/) on May 22, 2025. Retrieved November 9, 2025.
36. Orland, Kyle (December 6, 2024). "Google's Genie 2 "world model" reveal leaves more questions than answers" (https://web.archive.org/web/20241207000413/https://arstechnica.com/ai/2024/12/googles-genie-2-world-model-reveal-leaves-more-questions-than-answers/). *Ars Technica*. Archived from the original (https://arstechnica.com/ai/2024/12/googles-genie-2-world-model-reveal-leaves-more-questions-than-answers/) on December 7, 2024. Retrieved November 9, 2025.
37. Zeff, Maxwell (September 21, 2025). "Silicon Valley bets big on 'environments' to train AI agents" (https://web.archive.org/web/20250916191353/https://techcrunch.com/2025/09/16/silicon-valley-bets-big-on-environments-to-train-ai-agents/). *TechCrunch*. Archived from the original (https://techcrunch.com/2025/09/21/silicon-valley-bets-big-on-environments-to-train-ai-agents/) on September 16, 2025. Retrieved November 9, 2025.
38. Shazhaev, Ilman (November 24, 2025). "Why Game Engines Are Becoming A.I.'s Most Important Testbeds" (https://web.archive.org/web/20251203023639/https://observer.com/2025/11/gaming-training-next-gen-ai/). *Observer*. Archived from the original (https://observer.com/2025/11/gaming-training-next-gen-ai/) on December 3, 2025. Retrieved December 3, 2025.

39. David, Emilia (March 13, 2024). "Google's new AI will play video games with you — but not to win" (https://web.archive.org/web/20250602020104/https://www.theverge.com/2024/3/13/24099024/google-deepmind-ai-agent-sima-video-games). *The Verge*. Archived from the original (https://www.theverge.com/2024/3/13/24099024/google-deepmind-ai-agent-sima-video-games) on June 2, 2025. Retrieved December 3, 2025.
40. Metz, Cade (December 2, 2025). "Silicon Valley Builds Amazon and Gmail Copycats to Train A.I. Agents" (https://archive.ph/QsDWu). *The New York Times*. Archived from the original (https://www.nytimes.com/2025/12/02/technology/artificial-intelligence-amazon-gmail.html) on December 2, 2025. Retrieved December 2, 2025.
41. Colback, Lucy (May 7, 2025). "AI agents: from co-pilot to autopilot" (https://archive.today/20250507031905/https://www.ft.com/content/3e862e23-6e2c-4670-a68c-e204379fe01f). *Financial Times*. Archived from the original (https://www.ft.com/content/3e862e23-6e2c-4670-a68c-e204379fe01f) on May 7, 2025. Retrieved May 14, 2025.
42. Liu, Yue; Lo, Sin Kit; Lu, Qinghua; Zhu, Liming; Zhao, Dehai; Xu, Xiwei; Harrer, Stefan; Whittle, Jon (February 1, 2025). "Agent design pattern catalogue: A collection of architectural patterns for foundation model based agents" (https://www.sciencedirect.com/science/article/pii/S0164121224003224). *Journal of Systems and Software*. **220** 112278. doi:10.1016/j.jss.2024.112278 (https://doi.org/10.1016%2Fj.jss.2024.112278). ISSN 0164-1212 (https://search.worldcat.org/issn/0164-1212).
43. Masterman, Tula; Besen, Sandi; Sawtell, Mason; Chao, Alex (April 17, 2024), *The Landscape of Emerging AI Agent Architectures for Reasoning, Planning, and Tool Calling: A Survey* (http://arxiv.org/abs/2404.11584), arXiv:2404.11584 (https://arxiv.org/abs/2404.11584), retrieved December 3, 2025
44. Wray, Robert E.; Kirk, James R.; Laird, John E. (August 10, 2025). "Applying Cognitive Design Patterns to General LLM Agents" (https://doi.org/10.1007/978-3-032-00800-8_28). *Artificial General Intelligence*. Lecture Notes in Computer Science. Vol. 16058. Berlin, Heidelberg: Springer-Verlag. pp. 312–325. doi:10.1007/978-3-032-00800-8_28 (https://doi.org/10.1007%2F978-3-032-00800-8_28). ISBN 978-3-032-00799-5.
45. Knight, Will (September 25, 2024). "The Most Capable Open Source AI Model Yet Could Supercharge AI Agents" (https://web.archive.org/web/20250328102342/https://www.wired.com/story/molmo-open-source-multimodal-ai-model-allen-institute-agents/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/molmo-open-source-multimodal-ai-model-allen-institute-agents/) on March 28, 2025. Retrieved June 12, 2025.
46. Takahashi, Dean (November 4, 2024). "Nvidia AI Blueprint makes it easy for any devs to build automated agents that analyze video" (https://web.archive.org/web/20241205103955/https://venturebeat.com/ai/nvidia-ai-blueprint-makes-it-easy-for-devs-in-any-industry-build-agents-to-analyze-video/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/nvidia-ai-blueprint-makes-it-easy-for-devs-in-any-industry-build-agents-to-analyze-video/) on December 5, 2024. Retrieved June 12, 2025.
47. Takahashi, Dean (January 7, 2025). "Nvidia launches blueprint for AI agents that can analyze video" (https://web.archive.org/web/20250404224324/https://venturebeat.com/ai/nvidia-launches-blueprint-for-ai-agents-that-can-analyze-video/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/nvidia-launches-blueprint-for-ai-agents-that-can-analyze-video/) on April 4, 2025. Retrieved June 12, 2025.
48. Edwards, Benj (February 20, 2025). "Microsoft's new AI agent can control software and robots" (https://web.archive.org/web/20250520062232/https://arstechnica.com/ai/2025/02/microsofts-new-ai-agent-can-control-software-and-robots/). *Ars Technica*. Archived from the original (https://arstechnica.com/ai/2025/02/microsofts-new-ai-agent-can-control-software-and-robots/) on May 20, 2025. Retrieved June 12, 2025.

49. "Visa wants to give artificial intelligence 'agents' your credit card" (https://web.archive.org/web/20250501010808/https://apnews.com/article/ai-artificial-intelligence-5dfa1da145689e7951a181e2253ab349). *Associated Press*. April 30, 2025. Archived from the original (https://apnews.com/article/ai-artificial-intelligence-5dfa1da145689e7951a181e2253ab349) on May 1, 2025. Retrieved May 14, 2025.
50. Goldman, Sharon (June 11, 2025). "Microsoft Copilot flaw raises urgent questions for any business deploying AI agents" (https://web.archive.org/web/20250611235202/https://fortune.com/2025/06/11/microsoft-copilot-vulnerability-ai-agents-echoleak-hacking/). *Fortune*. Archived from the original (https://fortune.com/2025/06/11/microsoft-copilot-vulnerability-ai-agents-echoleak-hacking/) on June 11, 2025. Retrieved June 12, 2025.
51. Haskins, Caroline (May 2, 2025). "A DOGE Recruiter Is Staffing a Project to Deploy AI Agents Across the US Government" (https://web.archive.org/web/20250503074840/https://www.wired.com/story/doge-recruiter-ai-agents-palantir-clown-emoji/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/doge-recruiter-ai-agents-palantir-clown-emoji/) on May 3, 2025. Retrieved May 14, 2025.
52. Kachwala, Zaheer (August 18, 2025). "Nearly 90% of videogame developers use AI agents, Google study shows" (https://archive.today/20250818153431/https://www.reuters.com/business/nearly-90-videogame-developers-use-ai-agents-google-study-shows-2025-08-18/). *Reuters*. Archived from the original (https://www.reuters.com/business/nearly-90-videogame-developers-use-ai-agents-google-study-shows-2025-08-18/) on August 18, 2025. Retrieved November 9, 2025.
53. Knibbs, Kate (September 2, 2025). "Meet the Guys Betting Big on AI Gambling Agents" (https://web.archive.org/web/20250902112628/https://www.wired.com/story/sports-betting-crypto-artificial-intelligence-agents/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/sports-betting-crypto-artificial-intelligence-agents/) on September 2, 2025. Retrieved November 9, 2025.
54. Kharif, Olga (July 29, 2025). "Cornell Tech Professor Warns AI Agents And Crypto Spell Trouble" (https://archive.today/20250729233851/https://www.bloomberg.com/news/newsletters/2025-07-29/cornell-tech-professor-says-ai-agents-and-crypto-spell-trouble-bloomberg-crypto). *Bloomberg News*. Archived from the original (https://www.bloomberg.com/news/newsletters/2025-07-29/cornell-tech-professor-says-ai-agents-and-crypto-spell-trouble-bloomberg-crypto) on July 29, 2025. Retrieved November 9, 2025.
55. Herrman, John (August 22, 2025). "Why Everything's an AI 'Agent' Now" (https://web.archive.org/web/20250822141745/https://nymag.com/intelligencer/article/why-everything-is-an-ai-agent-now.html). *New York*. Archived from the original (https://nymag.com/intelligencer/article/why-everything-is-an-ai-agent-now.html) on August 22, 2025. Retrieved November 9, 2025.
56. Holmes, Aaron (October 21, 2025). "A Reality Check on Agents" (https://archive.today/20251022154702/https://www.theinformation.com/articles/reality-check-agents). *The Information*. Archived from the original (https://www.theinformation.com/articles/reality-check-agents) on October 22, 2025. Retrieved November 9, 2025.
57. "AI agents are coming for your privacy, warns Meredith Whittaker" (https://archive.today/20250916082648/https://www.economist.com/by-invitation/2025/09/09/ai-agents-are-coming-for-your-privacy-warns-meredith-whittaker). *The Economist*. September 9, 2025. ISSN 0013-0613 (https://search.worldcat.org/issn/0013-0613). Archived from the original (https://www.economist.com/by-invitation/2025/09/09/ai-agents-are-coming-for-your-privacy-warns-meredith-whittaker) on September 16, 2025. Retrieved November 9, 2025.
58. Cunningham, Andrew (November 18, 2025). "Microsoft tries to head off the "novel security risks" of Windows 11 AI agents" (https://archive.ph/jDmLO). *Ars Technica*. Archived from the original (https://arstechnica.com/gadgets/2025/11/new-windows-11-ai-agents-can-work-in-the-background-but-create-new-security-risks/) on November 19, 2025. Retrieved November 28, 2025.

59. Yang, Zeyi (December 4, 2025). "ByteDance and DeepSeek Are Placing Very Different AI Bets" (https://web.archive.org/web/20251205023422/https://www.wired.com/story/deepseek-goes-high-while-bytedance-goes-wide/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/deepseek-goes-high-while-bytedance-goes-wide/) on December 5, 2025. Retrieved December 11, 2025.
60. Chourasia, Ayush (December 8, 2025). "What is the TikTok owner's Agent AI phone? Find out why is it facing backlash in China" (https://web.archive.org/web/20251210032356/https://me.mashable.com/tech/64373/what-is-the-tiktok-owners-agent-ai-phone-find-out-why-is-it-facing-backlash-in-china). *Mashable*. Archived from the original (https://me.mashable.com/tech/64373/what-is-the-tiktok-owners-agent-ai-phone-find-out-why-is-it-facing-backlash-in-china) on December 10, 2025. Retrieved December 11, 2025.
61. Xu, Eunice (December 7, 2025). "ByteDance's agentic AI smartphone dials up a digital backlash by China's top apps" (https://archive.ph/JCM7G). *South China Morning Post*. Archived from the original (https://www.scmp.com/business/china-business/article/3335404/bytedances-agentic-ai-smartphone-dials-digital-backlash-chinas-top-apps) on December 7, 2025. Retrieved December 11, 2025.
62. Jiang, Ben (December 9, 2025). "Z.ai open sources AI agent tool for phones after ByteDance privacy backlash" (https://archive.ph/YS7XC). *South China Morning Post*. Archived from the original (https://www.scmp.com/tech/tech-trends/article/3335746/chinas-zai-open-sources-ai-agent-tool-phones-after-bytedance-privacy-backlash) on December 9, 2025. Retrieved December 11, 2025.
63. Rosenbush, Steven (November 12, 2025). "Companies Begin to See a Return on AI Agents" (https://archive.ph/D3ujh). *The Wall Street Journal*. ISSN 0099-9660 (https://search.worldcat.org/issn/0099-9660). Archived from the original (https://www.wsj.com/articles/companies-begin-to-see-a-return-on-ai-agents-671d830d) on November 12, 2025. Retrieved November 28, 2025.
64. Alms, Natalie (October 23, 2025). "As agencies shed staff, industry execs predict AI agents' rise" (https://archive.ph/v7dZU). *Government Executive*. Archived from the original (https://www.govexec.com/technology/2025/10/salesforce-pitches-ai-agents-government-sheds-staff/409017/) on December 7, 2025. Retrieved December 11, 2025.
65. Gold, Ashley (November 21, 2025). "Exclusive: IRS deploys AI agents" (https://archive.ph/iSCul). *Axios*. Archived from the original (https://www.axios.com/2025/11/21/irs-deploys-ai-agents) on November 21, 2025. Retrieved November 28, 2025.
66. Corrigan, Phil (November 26, 2025). "Staffordshire Police to trial AI 'agents' on 101 service" (https://archive.ph/OZnQk). *BBC*. Archived from the original (https://www.bbc.com/news/articles/cvgq03y0l3yo) on November 27, 2025. Retrieved November 28, 2025.
67. Aguilar, Mario (December 1, 2025). "FDA offers staff 'agentic AI' to support premarket reviews, administrative tasks" (https://web.archive.org/web/20251202002221/https://www.statnews.com/2025/12/01/fda-announces-agentic-ai-elsa-pre-merket-review/). *STAT*. Archived from the original (https://www.statnews.com/2025/12/01/fda-announces-agentic-ai-elsa-pre-merket-review/) on December 2, 2025. Retrieved December 6, 2025.
68. Losey, Stephen (December 9, 2025). "Pentagon taps Google Gemini, launches new site to boost AI use" (https://archive.ph/QbPvV). *Defense News*. Archived from the original (https://www.defensenews.com/pentagon/2025/12/09/pentagon-taps-google-gemini-launches-new-site-to-boost-ai-use/) on December 10, 2025. Retrieved December 11, 2025.
69. Zeff, Maxwell (July 9, 2025). "Perplexity launches Comet, an AI-powered web browser" (https://web.archive.org/web/20251010111103/https://techcrunch.com/2025/07/09/perplexity-launches-comet-an-ai-powered-web-browser/). *TechCrunch*. Archived from the original (https://techcrunch.com/2025/07/09/perplexity-launches-comet-an-ai-powered-web-browser/) on October 10, 2025. Retrieved December 1, 2025.
70. Roose, Kevin (February 1, 2025). "How Helpful Is Operator, OpenAI's New A.I. Agent?" (https://www.nytimes.com/2025/02/01/technology/openai-operator-agent.html). *The New York Times*. Retrieved August 9, 2025.

71. Warren, Tom (August 6, 2025). "Microsoft's plan to fix the web with AI has already hit an embarrassing security flaw" (https://www.theverge.com/news/719617/microsoft-nlweb-security-flaw-agentic-web). *The Verge*. Retrieved August 9, 2025.
72. Vekaria, Yash; Canino, Aurelio Loris; Levitsky, Jonathan; Ciechonski, Alex; Callejo, Patricia; Mandalari, Anna Maria; Shafiq, Zubair (June 10, 2025), *Big Help or Big Brother? Auditing Tracking, Profiling, and Personalization in Generative AI Assistants*, arXiv:2503.16586 (https://arxiv.org/abs/2503.16586)
73. Piper, Kelsey (March 29, 2024). "AI "agents" could do real work in the real world. That might not be a good thing" (https://web.archive.org/web/20241219213538/https://www.vox.com/future-perfect/24114582/artificial-intelligence-agents-openai-chatgpt-microsoft-google-ai-safety-risk-anthropic-claude). *Vox*. Archived from the original (https://www.vox.com/future-perfect/24114582/artificial-intelligence-agents-openai-chatgpt-microsoft-google-ai-safety-risk-anthropic-claude) on December 19, 2024. Retrieved January 14, 2025.
74. Purdy, Mark (December 12, 2024). "What Is Agentic AI, and How Will It Change Work?" (https://archive.today/20241230071722/https://hbr.org/2024/12/what-is-agentic-ai-and-how-will-it-change-work). *Harvard Business Review*. ISSN 0017-8012 (https://search.worldcat.org/issn/0017-8012). Archived from the original (https://hbr.org/2024/12/what-is-agentic-ai-and-how-will-it-change-work) on December 30, 2024. Retrieved January 20, 2025.
75. Wright, Webb (December 12, 2024). "AI Agents with More Autonomy Than Chatbots Are Coming. Some Safety Experts Are Worried" (https://web.archive.org/web/20241223010402/https://www.scientificamerican.com/article/what-are-ai-agents-and-why-are-they-about-to-be-everywhere/). *Scientific American*. Archived from the original (https://www.scientificamerican.com/article/what-are-ai-agents-and-why-are-they-about-to-be-everywhere/) on December 23, 2024. Retrieved January 14, 2025.
76. Olson, Parmy (January 27, 2025). "Skip the Hype, Here's How AI 'Agents' Can Really Help" (https://archive.today/20250127052332/https://www.bloomberg.com/opinion/articles/2025-01-27/skip-the-hype-here-s-how-ai-agents-can-really-help). *Bloomberg News*. Archived from the original (https://www.bloomberg.com/opinion/articles/2025-01-27/skip-the-hype-here-s-how-ai-agents-can-really-help) on January 27, 2025. Retrieved April 2, 2025.
77. Deng, Xiang; Gu, Yu; Zheng, Boyuan; Chen, Shijie; Stevens, Samuel; Wang, Boshi; Sun, Huan; Su, Yu (2023). "Mind2Web: Towards a Generalist Agent for the Web". arXiv:2306.06070 (https://arxiv.org/abs/2306.06070) [cs.CL (https://arxiv.org/archive/cs.CL)].
78. Woodall, Tatyana (January 9, 2024). "Researchers developing AI to make the internet more accessible" (https://web.archive.org/web/20250328092959/https://news.osu.edu/researchers-developing-ai-to-make-the-internet-more-accessible/). *Ohio State News*. Archived from the original (https://news.osu.edu/researchers-developing-ai-to-make-the-internet-more-accessible/) on March 28, 2025. Retrieved April 2, 2025.
79. Mitchell, Margaret; Ghosh, Avijit; Luccioni, Sasha; Pistilli, Giada (March 24, 2025). "Why handing over total control to AI agents would be a huge mistake" (https://web.archive.org/web/20250324115123/https://www.technologyreview.com/2025/03/24/1113647/why-handing-over-total-control-to-ai-agents-would-be-a-huge-mistake/). *MIT Technology Review*. Archived from the original (https://www.technologyreview.com/2025/03/24/1113647/why-handing-over-total-control-to-ai-agents-would-be-a-huge-mistake/) on March 24, 2025. Retrieved April 2, 2025.
80. "AI agents: Exploring the potential and the problems" (https://web.archive.org/web/20250610134839/https://www.bbc.co.uk/rd/articles/2025-05-ai-agents-challenges-summary). *BBC Online*. May 30, 2025. Archived from the original (https://www.bbc.co.uk/rd/articles/2025-05-ai-agents-challenges-summary) on June 10, 2025. Retrieved June 12, 2025.

81. Porter, Eduardo (October 23, 2025). "Once the AI bubble pops, we'll all suffer. Could that be better than letting it grow unabated?" (https://archive.today/20251023160756/https://www.theguardian.com/technology/2025/oct/23/ai-bubble-economy-workers-wage-growth). *The Guardian*. ISSN 0261-3077 (https://search.worldcat.org/issn/0261-3077). Archived from the original (https://www.theguardian.com/technology/2025/oct/23/ai-bubble-economy-workers-wage-growth) on October 23, 2025. Retrieved November 9, 2025.
82. O'Neill, Brian (December 18, 2024). "What is an AI agent? A computer scientist explains the next wave of artificial intelligence tools" (https://web.archive.org/web/20250104000722/https://theconversation.com/what-is-an-ai-agent-a-computer-scientist-explains-the-next-wave-of-artificial-intelligence-tools-242586). *The Conversation*. Archived from the original (https://theconversation.com/what-is-an-ai-agent-a-computer-scientist-explains-the-next-wave-of-artificial-intelligence-tools-242586) on January 4, 2025. Retrieved January 14, 2025.
83. "AI agents: Exploring the potential and the problems" (https://web.archive.org/web/20250610134839/https://www.bbc.co.uk/rd/articles/2025-05-ai-agents-challenges-summary). *BBC Online*. May 30, 2025. Archived from the original (https://www.bbc.co.uk/rd/articles/2025-05-ai-agents-challenges-summary) on June 10, 2025. Retrieved June 12, 2025.
84. Huckins, Grace (June 12, 2025). "Are we ready to hand AI agents the keys?" (https://web.archive.org/web/20250612113313/https://www.technologyreview.com/2025/06/12/1118189/ai-agents-manus-control-autonomy-operator-openai/). *MIT Technology Review*. Archived from the original (https://www.technologyreview.com/2025/06/12/1118189/ai-agents-manus-control-autonomy-operator-openai/) on June 12, 2025. Retrieved June 15, 2025.
85. Lin, Belle (January 6, 2025). "How Are Companies Using AI Agents? Here's a Look at Five Early Users of the Bots" (https://archive.today/20250106123337/https://www.wsj.com/articles/how-are-companies-using-ai-agents-heres-a-look-at-five-early-users-of-the-bots-26f87845). *The Wall Street Journal*. ISSN 0099-9660 (https://search.worldcat.org/issn/0099-9660). Archived from the original (https://www.wsj.com/articles/how-are-companies-using-ai-agents-heres-a-look-at-five-early-users-of-the-bots-26f87845) on January 6, 2025. Retrieved January 20, 2025.
86. Zittrain, Jonathan L. (July 2, 2024). "We Need to Control AI Agents Now" (https://web.archive.org/web/20241231080834/https://www.theatlantic.com/technology/archive/2024/07/ai-agents-safety-risks/678864/). *The Atlantic*. Archived from the original (https://www.theatlantic.com/technology/archive/2024/07/ai-agents-safety-risks/678864/) on December 31, 2024. Retrieved January 20, 2025.
87. Kerner, Sean Michael (January 16, 2025). "Nvidia tackles agentic AI safety and security with new NeMo Guardrails NIMs" (https://web.archive.org/web/20250116161332/https://venturebeat.com/ai/nvidia-boosts-agentic-ai-safety-with-nemo-guardrails-promising-better-protection-with-low-latency/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/nvidia-boosts-agentic-ai-safety-with-nemo-guardrails-promising-better-protection-with-low-latency/) on January 16, 2025. Retrieved January 20, 2025.
88. Silva, Daswin de (July 27, 2025). "AI agents are here. Here's what to know about what they can do – and how they can go wrong" (https://web.archive.org/web/20250728112639/https://theconversation.com/ai-agents-are-here-heres-what-to-know-about-what-they-can-do-and-how-they-can-go-wrong-261579). *The Conversation*. Archived from the original (https://theconversation.com/ai-agents-are-here-heres-what-to-know-about-what-they-can-do-and-how-they-can-go-wrong-261579) on July 28, 2025. Retrieved November 9, 2025.
89. Crawford, Kate (December 23, 2024). "AI Agents Will Be Manipulation Engines" (https://web.archive.org/web/20250103053608/https://www.wired.com/story/ai-agents-personal-assistants-manipulation-engines/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/ai-agents-personal-assistants-manipulation-engines/) on January 3, 2025. Retrieved January 14, 2025.

90. Wright, Webb (December 12, 2024). "AI Agents with More Autonomy Than Chatbots Are Coming. Some Safety Experts Are Worried" (https://web.archive.org/web/20241223010402/https://www.scientificamerican.com/article/what-are-ai-agents-and-why-are-they-about-to-be-everywhere/). *Scientific American*. Archived from the original (https://www.scientificamerican.com/article/what-are-ai-agents-and-why-are-they-about-to-be-everywhere/) on December 23, 2024. Retrieved January 14, 2025.
91. Blackman, Reid (June 13, 2025). "Organizations Aren't Ready for the Risks of Agentic AI" (https://archive.today/20250613122927/https://hbr.org/2025/06/organizations-arent-ready-for-the-risks-of-agentic-ai). *Harvard Business Review*. ISSN 0017-8012 (https://search.worldcat.org/issn/0017-8012). Archived from the original (https://hbr.org/2025/06/organizations-arent-ready-for-the-risks-of-agentic-ai) on June 13, 2025. Retrieved June 15, 2025.
92. "We did the math on AI's energy footprint. Here's the story you haven't heard" (https://web.archive.org/web/20250520105527/https://www.technologyreview.com/2025/05/20/1116327/ai-energy-usage-climate-footprint-big-tech/). *MIT Technology Review*. May 20, 2025. Archived from the original (https://www.technologyreview.com/2025/05/20/1116327/ai-energy-usage-climate-footprint-big-tech/) on May 20, 2025. Retrieved June 12, 2025. "We started small, as the question of how much a single query costs is vitally important to understanding the bigger picture. That's because those queries are being built into ever more applications beyond standalone chatbots: from search, to agents, to the mundane daily apps we use to track our fitness, shop online, or book a flight. The energy resources required to power this artificial-intelligence revolution are staggering, and the world's biggest tech companies have made it a top priority to harness ever more of that energy, aiming to reshape our energy grids in the process."
93. "Inside the effort to tally AI's energy appetite" (https://web.archive.org/web/20250603110116/https://www.technologyreview.com/2025/06/03/1117685/inside-the-tedious-effort-to-tally-ais-energy-appetite/). *MIT Technology Review*. June 3, 2025. Archived from the original (https://www.technologyreview.com/2025/06/03/1117685/inside-the-tedious-effort-to-tally-ais-energy-appetite/) on June 3, 2025. Retrieved June 12, 2025. "Lots of AI companies are building reasoning models, which "think" for longer and use more energy. They're building hardware devices, perhaps like the one Jony Ive has been working on (which OpenAI just acquired for $6.5 billion), that have AI constantly humming along in the background of our conversations. They're designing agents and digital clones of us to act on our behalf. All these trends point to a more energy-intensive future (which, again, helps explain why OpenAI and others are spending such inconceivable amounts of money on energy)."
94. Levy, Steven (June 20, 2025). "What Big Tech's Band of Execs Will Do in the Army" (https://web.archive.org/web/20250620143355/https://www.wired.com/story/what-lt-col-boz-and-big-techs-enlisted-execs-will-do-in-the-army/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/what-lt-col-boz-and-big-techs-enlisted-execs-will-do-in-the-army/) on June 20, 2025. Retrieved November 9, 2025.
95. Wong, Matteo (March 14, 2025). "Was Sam Altman Right About the Job Market?" (https://web.archive.org/web/20250317115042/https://www.theatlantic.com/technology/archive/2025/03/generative-ai-agents/682050/). *The Atlantic*. Archived from the original (https://www.theatlantic.com/technology/archive/2025/03/generative-ai-agents/682050/) on March 17, 2025. Retrieved April 2, 2025. "In other words, flawed products won't stop tech companies' push to automate everything—the AI-saturated future will be imperfect at best, but it is coming anyway."
96. Agarwal, Shubham. "Carnegie Mellon staffed a fake company with AI agents. It was a total disaster" (https://web.archive.org/web/20250428031158/https://www.businessinsider.com/ai-agents-study-company-run-by-ai-disaster-replace-jobs-2025-4). *Business Insider*. Archived from the original (https://www.businessinsider.com/ai-agents-study-company-run-by-ai-disaster-replace-jobs-2025-4) on April 28, 2025. Retrieved May 15, 2025.

97. Sabin, Sam (April 22, 2025). "Exclusive: Anthropic warns fully AI employees are a year away" (https://web.archive.org/web/20250423000910/https://www.axios.com/2025/04/22/ai-anthropic-virtual-employees-security). *Axios*. Archived from the original (https://www.axios.com/2025/04/22/ai-anthropic-virtual-employees-security) on April 23, 2025. Retrieved May 15, 2025.
98. Xu, Frank F.; Song, Yufan; Li, Boxuan; Tang, Yuxuan; Jain, Kritanjali; Bao, Mengxue; Wang, Zora Z.; Zhou, Xuhui; Guo, Zhitong; Cao, Murong; Yang, Mingyang; Hao Yang Lu; Martin, Amaad; Su, Zhe; Maben, Leander; Mehta, Raj; Chi, Wayne; Jang, Lawrence; Xie, Yiqing; Zhou, Shuyan; Neubig, Graham (2024). "TheAgentCompany: Benchmarking LLM Agents on Consequential Real World Tasks". arXiv:2412.14161 (https://arxiv.org/abs/2412.14161) [cs.CL (https://arxiv.org/archive/cs.CL)].
99. Claburn, Thomas (January 23, 2025). "Tool touted as 'first AI software engineer' is bad at its job, testers claim" (https://web.archive.org/web/20250330003601/https://www.theregister.com/2025/01/23/ai_developer_devin_poor_reviews/). *The Register*. Archived from the original (https://www.theregister.com/2025/01/23/ai_developer_devin_poor_reviews/) on March 30, 2025. Retrieved June 15, 2025.
100. Clark, Lindsay (June 16, 2025). "Salesforce study finds LLM agents flunk CRM and confidentiality tests" (https://web.archive.org/web/20250616144144/https://www.theregister.com/2025/06/16/salesforce_llm_agents_benchmark/). *The Register*. Archived from the original (https://www.theregister.com/2025/06/16/salesforce_llm_agents_benchmark/) on June 16, 2025. Retrieved November 9, 2025.
101. Huang, Kung-Hsiang; Prabhakar, Akshara; Thorat, Onkar; Agarwal, Divyansh; Choubey, Prafulla Kumar; Mao, Yixin; Savarese, Silvio; Xiong, Caiming; Wu, Chien-Sheng (May 24, 2025), *CRMArena-Pro: Holistic Assessment of LLM Agents Across Diverse Business Scenarios and Interactions* (https://web.archive.org/web/20250613074306/http://arxiv.org/abs/2505.18878), arXiv:2505.18878 (https://arxiv.org/abs/2505.18878), archived from the original (http://arxiv.org/abs/2505.18878) on June 13, 2025, retrieved November 9, 2025
102. Knight, Will (October 29, 2025). "AI Agents Are Terrible Freelance Workers" (https://archive.today/20251102151118/https://www.wired.com/story/ai-agents-are-terrible-freelance-workers/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/ai-agents-are-terrible-freelance-workers/) on November 2, 2025. Retrieved November 9, 2025.
103. Morrow, Allison (June 18, 2025). "AI warnings are the hip new way for CEOs to keep their workers afraid of losing their jobs" (https://web.archive.org/web/20250618185619/https://www.cnn.com/2025/06/18/business/ai-warnings-ceos). *CNN*. Archived from the original (https://www.cnn.com/2025/06/18/business/ai-warnings-ceos) on June 18, 2025. Retrieved November 9, 2025.
104. Hart, Jordan. "Coinbase CEO says he 'went rogue' and fired some employees who didn't adopt AI after being told to" (https://web.archive.org/web/20250821174356/https://www.businessinsider.com/coinbase-ceo-fired-employees-not-using-ai-tools-onboarding-2025-8). *Business Insider*. Archived from the original (https://www.businessinsider.com/coinbase-ceo-fired-employees-not-using-ai-tools-onboarding-2025-8) on August 21, 2025. Retrieved November 9, 2025.
105. Langley, Hugh. "For Googlers, the pressure is on to use AI for everything — or get left behind" (https://web.archive.org/web/20250821132636/https://www.businessinsider.com/google-employees-use-ai-or-get-left-behind-gemini-2025-8). *Business Insider*. Archived from the original (https://www.businessinsider.com/google-employees-use-ai-or-get-left-behind-gemini-2025-8) on August 21, 2025. Retrieved November 9, 2025.
106. Landymore, Frank (October 22, 2025). "AWS Outage That Took Down Internet Came After Amazon Fired Tons of Workers in Favor of AI" (https://archive.today/20251024195032/https://futurism.com/artificial-intelligence/aws-outage-amazon-fired-workers-ai). *Futurism*. Archived from the original (https://futurism.com/artificial-intelligence/aws-outage-amazon-fired-workers-ai) on October 24, 2025. Retrieved November 9, 2025.

107. Balevic, Katie. "Signal president warns the hyped agentic AI bots threaten user privacy" (https://web.archive.org/web/20250312185602/https://www.businessinsider.com/signal-president-warns-privacy-threat-agentic-ai-meredith-whittaker-2025-3). *Business Insider*. Archived from the original (https://www.businessinsider.com/signal-president-warns-privacy-threat-agentic-ai-meredith-whittaker-2025-3) on March 12, 2025. Retrieved April 2, 2025.
108. Hornstein, Julia. "AI agents are coming to the military. VCs love it, but researchers are a bit wary" (https://web.archive.org/web/20250312101554/https://www.businessinsider.com/ai-agents-coming-military-new-scaleai-contract-2025-3). *Business Insider*. Archived from the original (https://www.businessinsider.com/ai-agents-coming-military-new-scaleai-contract-2025-3) on March 12, 2025. Retrieved April 2, 2025.
109. Regalbuto, Gabriele (July 28, 2025). "Former Army officer develops offline AI for military use as Pentagon funds tech giants" (https://web.archive.org/web/20250728200822/https://www.foxbusiness.com/technology/former-army-officer-develops-offline-ai-military-use-pentagon-funds-tech-giants). *Fox Business*. Archived from the original (https://www.foxbusiness.com/technology/former-army-officer-develops-offline-ai-military-use-pentagon-funds-tech-giants) on July 28, 2025. Retrieved November 9, 2025.
110. Tangermann, Victor (March 6, 2025). "Pentagon Signs Deal to "Deploy AI Agents for Military Use" " (https://web.archive.org/web/20250308022255/https://futurism.com/pentagon-signs-deal-deploy-ai-agents-military-use). *Futurism*. Archived from the original (https://futurism.com/pentagon-signs-deal-deploy-ai-agents-military-use) on March 8, 2025. Retrieved April 2, 2025.
111. Jensen, Benjamin (March 4, 2025). "The Troubling Truth About How AI Agents Act in a Crisis" (https://archive.today/20250304114949/https://foreignpolicy.com/2025/03/04/ai-bias-national-security-study/). *Foreign Policy*. Archived from the original (https://foreignpolicy.com/2025/03/04/ai-bias-national-security-study/) on March 4, 2025. Retrieved April 2, 2025.
112. Nuñez, Michael (February 25, 2025). "OpenAI expands Deep Research access to Plus users, heating up AI agent wars with DeepSeek and Claude" (https://web.archive.org/web/20250311120439/https://venturebeat.com/ai/openai-expands-deep-research-access-to-plus-users-heating-up-ai-agent-wars-with-deepseek-and-claude/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/openai-expands-deep-research-access-to-plus-users-heating-up-ai-agent-wars-with-deepseek-and-claude/) on March 11, 2025. Retrieved April 2, 2025.
113. Herrman, John (January 25, 2025). "What Are AI 'Agents' For?" (https://web.archive.org/web/20250125112442/https://nymag.com/intelligencer/article/what-are-ai-agents-like-openai-operator-for.html). *Intelligencer*. Archived from the original (https://nymag.com/intelligencer/article/what-are-ai-agents-like-openai-operator-for.html) on January 25, 2025. Retrieved April 2, 2025.
114. Herrman, John (December 6, 2025). "How AI Companies Are Simulating the Robot Takeover" (https://archive.ph/zz3Nh). *Intelligencer*. Archived from the original (https://nymag.com/intelligencer/article/how-ai-companies-are-simulating-the-robot-takeover.html) on December 6, 2025. Retrieved December 6, 2025.
115. Caramela, Sammi (February 1, 2025). " 'Dead Internet Theory' Is Back Thanks to All of That AI Slop" (https://web.archive.org/web/20250201192805/https://www.vice.com/en/article/dead-internet-theory-is-back-thanks-to-all-of-that-ai-slop/). *VICE*. Archived from the original (https://www.vice.com/en/article/dead-internet-theory-is-back-thanks-to-all-of-that-ai-slop/) on February 1, 2025. Retrieved April 2, 2025.
116. Metz, Cade; Weise, Karen (October 16, 2023). "How 'A.I. Agents' That Roam the Internet Could One Day Replace Workers" (https://archive.today/20231219182907/https://www.nytimes.com/2023/10/16/technology/ai-agents-workers-replace.html). *The New York Times*. ISSN 0362-4331 (https://search.worldcat.org/issn/0362-4331). Archived from the original (https://www.nytimes.com/2023/10/16/technology/ai-agents-workers-replace.html) on December 19, 2023. Retrieved April 2, 2025.

117. Ming, Lee Chong. "Replit's CEO apologizes after its AI agent wiped a company's code base in a test run and lied about it" (https://web.archive.org/web/20251007174914/https://www.businessinsider.com/replit-ceo-apologizes-ai-coding-tool-delete-company-database-2025-7). *Business Insider*. Archived from the original (https://www.businessinsider.com/replit-ceo-apologizes-ai-coding-tool-delete-company-database-2025-7) on October 7, 2025. Retrieved November 9, 2025.
118. Edwards, Benj (July 24, 2025). "Two major AI coding tools wiped out user data after making cascading mistakes" (https://web.archive.org/web/20250725193539/https://arstechnica.com/information-technology/2025/07/ai-coding-assistants-chase-phantoms-destroy-real-user-data/). *Ars Technica*. Archived from the original (https://arstechnica.com/information-technology/2025/07/ai-coding-assistants-chase-phantoms-destroy-real-user-data/) on July 25, 2025. Retrieved November 9, 2025.
119. Morales, Jowi (December 3, 2025). "Google's Agentic AI wipes user's entire HDD without permission in catastrophic failure — cache wipe turns into mass deletion event as agent apologizes: "I am absolutely devastated to hear this. I cannot express how sorry I am" " (https://web.archive.org/web/20251204162610/https://www.tomshardware.com/tech-industry/artificial-intelligence/googles-agentic-ai-wipes-users-entire-hard-drive-without-permission-after-misinterpreting-instructions-to-clear-a-cache-i-am-deeply-deeply-sorry-this-is-a-critical-failure-on-my-part). *Tom's Hardware*. Archived from the original (https://www.tomshardware.com/tech-industry/artificial-intelligence/googles-agentic-ai-wipes-users-entire-hard-drive-without-permission-after-misinterpreting-instructions-to-clear-a-cache-i-am-deeply-deeply-sorry-this-is-a-critical-failure-on-my-part) on December 4, 2025. Retrieved December 6, 2025.
120. Williams, Tom (July 24, 2025). "Is the new ChatGPT agent really a weapons risk?" (https://web.archive.org/web/20250729102556/https://ia.acs.org.au/article/2025/is-the-new-chatgpt-agent-really-a-weapons-risk-.html). *Information Age*. Archived from the original (https://ia.acs.org.au/article/2025/is-the-new-chatgpt-agent-really-a-weapons-risk-.html) on July 29, 2025. Retrieved November 9, 2025.
121. Franzen, Carl (July 31, 2025). "You've heard of AI 'Deep Research' tools…now Manus is launching 'Wide Research' that spins up 100+ agents to scour the web for you" (http://web.archive.org/web/20250822091624/https://venturebeat.com/ai/youve-heard-of-ai-deep-research-tools-now-manus-is-launching-wide-research-that-spins-up-100-agents-to-scour-the-web-for-you/). *VentureBeat*. Archived from the original (https://venturebeat.com/ai/youve-heard-of-ai-deep-research-tools-now-manus-is-launching-wide-research-that-spins-up-100-agents-to-scour-the-web-for-you/) on August 22, 2025. Retrieved November 9, 2025.
122. Goodin, Dan (November 14, 2025). "Researchers question Anthropic claim that AI-assisted attack was 90% autonomous" (https://web.archive.org/web/20251126014220/https://arstechnica.com/security/2025/11/researchers-question-anthropic-claim-that-ai-assisted-attack-was-90-autonomous/). *Ars Technica*. Archived from the original (https://arstechnica.com/security/2025/11/researchers-question-anthropic-claim-that-ai-assisted-attack-was-90-autonomous/) on November 26, 2025. Retrieved November 28, 2025.
123. Down, Aisha (November 14, 2025). "AI firm claims it stopped Chinese state-sponsored cyber-attack campaign" (https://archive.ph/dWm7Z). *The Guardian*. ISSN 0261-3077 (https://search.worldcat.org/issn/0261-3077). Archived from the original (https://www.theguardian.com/technology/2025/nov/14/ai-anthropic-chinese-state-sponsored-cyber-attack) on November 14, 2025. Retrieved November 28, 2025.
124. Nolan, Beatrice (November 27, 2025). "Signal's president warns AI agents are an existential threat to secure messaging apps" (https://archive.ph/Dva2q). *Fortune*. Archived from the original (https://fortune.com/2025/11/27/ai-agents-are-an-existential-threat-to-secure-messaging-signals-president-whittaker-says/) on November 27, 2025. Retrieved November 28, 2025.

125. Knight, Will (April 9, 2025). "The AI Agent Era Requires a New Kind of Game Theory" (https://web.archive.org/web/20250409202024/https://www.wired.com/story/zico-kolter-ai-agents-game-theory/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/zico-kolter-ai-agents-game-theory/) on April 9, 2025. Retrieved May 15, 2025.

126. Varanasi, Lakshmi. "Don't get too excited about AI agents yet. They make a lot of mistakes" (https://web.archive.org/web/20250418101155/https://www.businessinsider.com/ai-agents-errors-hallucinations-compound-risk-2025-4). *Business Insider*. Archived from the original (https://www.businessinsider.com/ai-agents-errors-hallucinations-compound-risk-2025-4) on April 18, 2025. Retrieved May 15, 2025.

127. Shah, Agam (July 21, 2025). "As AI agents go mainstream, companies lean into confidential computing for data security" (https://web.archive.org/web/20250722081702/https://www.computerworld.com/article/4025903/as-ai-agents-go-mainstream-companies-lean-into-confidential-computing-for-data-security.html). *Computerworld*. Archived from the original (https://www.computerworld.com/article/4025903/as-ai-agents-go-mainstream-companies-lean-into-confidential-computing-for-data-security.html) on July 22, 2025. Retrieved November 9, 2025.

128. Belcak, Peter; Heinrich, Greg; Diao, Shizhe; Fu, Yonggan; Dong, Xin; Muralidharan, Saurav; Lin, Yingyan Celine; Molchanov, Pavlo (September 15, 2025), *Small Language Models are the Future of Agentic AI* (https://web.archive.org/web/20251004033726/https://arxiv.org/abs/2506.02153), arXiv:2506.02153 (https://arxiv.org/abs/2506.02153), archived from the original (http://arxiv.org/abs/2506.02153) on October 4, 2025, retrieved November 9, 2025

129. Blum, Sam (August 12, 2025). "Did Sam Altman Accidentally Admit That the AI Bubble Is Here?" (http://web.archive.org/web/20250830144426/https://www.inc.com/sam-blum/sam-altman-open-ai-bubble-is-here/91226419). *Inc.* Archived from the original (https://www.inc.com/sam-blum/sam-altman-open-ai-bubble-is-here/91226419) on August 30, 2025. Retrieved November 9, 2025.

130. "Why AI systems may never be secure, and what to do about it" (https://archive.today/20251011102639/https://www.economist.com/science-and-technology/2025/09/22/why-ai-systems-may-never-be-secure-and-what-to-do-about-it). *The Economist*. September 22, 2025. ISSN 0013-0613 (https://search.worldcat.org/issn/0013-0613). Archived from the original (https://www.economist.com/science-and-technology/2025/09/22/why-ai-systems-may-never-be-secure-and-what-to-do-about-it) on October 11, 2025. Retrieved November 9, 2025.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Agentic_AI&oldid=1326889178"