

Google's Gemini agent launches as UK watchdog flags AI risks

Executive Summary

Google took a major step into autonomous enterprise AI on 8 October by launching its new Gemini agent for work, an AI "coworker" that can act across business applications. Meanwhile regulators and vendors are sharpening their focus on the safety and accountability of these autonomous tools, introducing new rules and technologies to ensure AI agents can be deployed securely and with measurable results

Google's Gemini agent enters enterprise workflows

Google this week unveiled the Gemini agent, a new AI system aimed at working alongside employees to automate a range of business tasks. Announced at a Google Cloud event on 8 October, the Gemini agent is a single AI "coworker" designed to handle knowledge work, content creation, coding and more tasks from one interface (techcrunch.com [1]). Unlike traditional chatbots, it is built to take actions on a user's behalf: CEO Thomas Kurian said the agent can be given broad "objectives" instead of step-by-step instructions, allowing it to plan workflows, use specialised tools and connect to internal business systems to accomplish its goals (techcrunch.com [2]). The agent also integrates with other software that companies already use, working within Google Workspace apps and even connecting to outside platforms like Microsoft 365, Slack and Salesforce to complete multi-step tasks (techcrunch.com [3]).

Google's move underscores how far AI agents have come in businesses this year. The company is initially rolling out Gemini to its enterprise customers, after noting that nearly 90% of Fortune 100 firms already use its Gemini AI models (techcrunch.com [4]). It follows OpenAI's September release of always-on "dot" agents and Meta's introduction of its "Muse" shopping agent (www.cnbc.com [5]), as big tech firms compete to offer AI agents that go beyond answering questions to performing real work. For enterprise leaders, Google's entry means the competition is producing ever more capable AI assistants that can automate routine processes across common workplace apps. This raises new opportunities to streamline workflows, but also puts pressure on organisations to have the right infrastructure and policies to manage these autonomous systems responsibly

References:

- [1] techcrunch.com — <https://techcrunch.com/2026/10/08/google-brings-agentic-ai-to-gemini-starting-with-businesses/#:~:text=Sarah%20Perez%2011%3A18%20AM%20PDT,The%20move%20comes%20as>
- [2] techcrunch.com — <https://techcrunch.com/2026/10/08/google-brings-agentic-ai-to-gemini-starting-with-businesses/#:~:text=these,include%20attachments%2C%20like%20files%2C%20folders>
- [3] techcrunch.com — <https://techcrunch.com/2026/10/08/google-brings-agentic-ai-to-gemini-starting-with-businesses/#:~:text=will%20expand%20the%20model%20picker,is%20doing%20from%20a%20%E2%80%9Ctasks>
- [4] techcrunch.com — <https://techcrunch.com/2026/10/08/google-brings-agentic-ai-to-gemini-starting-with-businesses/#:~:text=monthly%20active%20users,connect%20to%20businesses%E2%80%99%20internal%20systems>
- [5] www.cnbc.com — <https://www.cnbc.com/2026/10/08/google-cloud-introduces-gemini-agent-for-work-as-ai-race-heats-up.html#:~:text=answer%20questions%2C%20handle%20tasks%2C%20create,The>

Regulators turn attention to agentic AI

As AI agents move into live operations, regulators are stepping in to address the potential risks. On 8 October, the UK's data protection authority (the Information Commissioner's Office, or ICO) announced that it had secured commitments from ten major AI developers to improve their data safeguards and transparency after a period of regulatory scrutiny (ico.org.uk [1]). The watchdog simultaneously launched a six-week "call for evidence" on the data protection issues posed by "agentic AI" - autonomous AI systems that make decisions and take actions with minimal human involvement (ico.org.uk [2]). The regulator also confirmed it is looking into recent experimental deployments of AI agents to evaluate their compliance with privacy laws (ico.org.uk [3]).

This marks one of the first major regulatory moves targeting autonomous AI. It signals that companies designing or using AI agents will need to prove robust controls over the data their systems ingest and produce. Businesses deploying such “digital worker” agents should prepare for new oversight, ensuring that any AI agent working on customer data is auditable and adheres to privacy and security requirements. Regulatory attention is catching up with the rapid expansion of agent capabilities, making trustworthy design and thorough testing a prerequisite for scaling autonomous workflows

References:

[1] [ico.org.uk — https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/10/ico-secures-changes-from-leading-ai-developers-as-scrutiny-extends-to-ai-agents/](https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/10/ico-secures-changes-from-leading-ai-developers-as-scrutiny-extends-to-ai-agents/)

#::~text=Type%20News%20Ten%20leading%20AI,around%20recent%20agentic%20AI%20testing

[2] [ico.org.uk — https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/10/ico-secures-changes-from-leading-ai-developers-as-scrutiny-extends-to-ai-agents/](https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/10/ico-secures-changes-from-leading-ai-developers-as-scrutiny-extends-to-ai-agents/)

#::~text=Type%20News%20Ten%20leading%20AI,around%20recent%20agentic%20AI%20testing

[3] [ico.org.uk — https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/10/ico-secures-changes-from-leading-ai-developers-as-scrutiny-extends-to-ai-agents/](https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/10/ico-secures-changes-from-leading-ai-developers-as-scrutiny-extends-to-ai-agents/)

#~:~text=Type%20News%20Ten%20leading%20AI.around%20recent%20agentic%20AI%20testing

Building reliability into autonomous workflows

Technology providers are also rolling out solutions to help enterprises manage AI agents more safely and effectively. On 12 October, cloud platform DigitalOcean announced new “Agent Data” and “Agent Learning” services to improve AI agents’ ability to learn from their own actions and errors. The offerings provide a dedicated data layer for agents to access and record relevant context, along with tools to capture agent decisions, flag failure modes like inaccuracies, and test fixes before deployment. By providing a built-in feedback loop for autonomous systems, the aim is to shorten the time it takes to identify and correct a misbehaving agent, reducing the risk of errors in production.

This move highlights a broader industry trend of fortifying AI agents with guardrails and performance monitoring. Just as Microsoft and startups like Tulip recently introduced “sandbox” environments to contain agent actions, DigitalOcean’s approach focuses on continuous improvement: giving AI agents a mechanism to self-monitor and update their behaviour over time. For enterprises, such developments could lower the barrier to automating complex workflows by ensuring that agents remain reliable and compliant. The emphasis is shifting from whether AI agents can be launched to how well their performance can be measured and improved with each run

Key Statistics

- 20% - Increase in JPMorgan's private banking gross sales due to AI tools (JPMorgan CEO)
- 45% - Finance AI projects focused on productivity gains (Gartner, 2026 survey)
- 73% - UK CFOs optimistic AI will improve business performance (Deloitte, 2026 survey)
- 80% - Organisations say AI agent investments already deliver returns (Anthropic, 2026 survey)

- 40% - Large enterprises (>\$1B revenue) scaling AI agents in 2026 (McKinsey survey)

KEY TAKEAWAY

Leaders should ensure any AI agents in use have explicit guardrails and monitoring. New tools can help track agent actions and performance, but compliance checks and human oversight remain essential

Sources

Google brings agentic AI to Gemini, starting with businesses

<https://techcrunch.com/2026/10/08/google-brings-agentic-ai-to-gemini-starting-with-businesses/>

Google Cloud introduces Gemini agent for work as AI race heats up

<https://money.usnews.com/investing/news/articles/2026-10-08/google-cloud-introduces-gemini-agent-for-work-as-ai-race-heats-up>

ICO secures changes from leading AI developers as scrutiny extends to AI agents

<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/10/ico-secures-changes-from-leading-ai-developers-as-scrutiny-extends-to-ai-agents/>

JPMorgan Chase AI: Bank to deploy more powerful agents this year

<https://www.cnbc.com/2026/06/09/jpmorgan-chase-ai-agents.html>

Gartner survey shows 45% of CFOs say their AI investments lean toward productivity

<https://www.gartner.com/en/newsroom/press-releases/2026-07-20-gartner-survey-shows-45-percent-of-cfos-say-their-ai-investments-lean-towards-productivity-while-20-percent-say-these-investments-lean-towards-decision-quality>

Deloitte CFO Survey Q2 2026: Growing AI optimism

<https://www.deloitte.com/uk/en/about/press-room/deloitte-cfo-survey-quater-two-2026-growing-ai-optimism.html>

How enterprises are building AI agents in 2026

<https://claude.com/resources/articles/how-enterprises-are-building-ai-agents-in-2026>

The state of AI in 2026: On the road to ROI

<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>

DigitalOcean launches agent data and learning services for AI

<https://www.hpcwire.com>

