Agents inside your governance: Bedrock Managed Agents and AgentCore Runtime

10 November 2026 · 5 min read · blogs.iictp.org/running-agents-under-existing-governance-bedrock-agentcore

Where an agent runs decides whose rules it runs under. Two AWS announcements from recent weekly roundups are examples of vendors answering that question.

TL;DR The short version

- Where an agent runs decides whose rules it runs under, and AWS's Bedrock Managed Agents preview and AgentCore Runtime are examples of vendors answering that.
- An agent running under your identity and permission system inherits your controls on access, logging and data location.
- Give each agent its own least-privilege identity, never reuse a person's credentials, and log every tool call.

Read online, listen to it, or change the text size: https://blogs.iictp.org/running-agents-under-existing-governance-bedrock-agentcore

What was reported

- On 5 October AWS described a public preview of Amazon Bedrock Managed Agents powered by OpenAI, built on a customised version of OpenAI's Agents API. AWS says you can build agents that run entirely inside AWS, with the identities, permissions and governance controls you already use.
- AWS lists two execution options: self-hosted compute, or Amazon Bedrock AgentCore Runtime for managed sessions.
- On 9 November AWS described an update to AgentCore Runtime in which, it says, sessions start small, page in more memory on demand, and give it back when cold instead of holding the peak. It frames the change as a single field on a runtime you already have.

Why the location matters

An agent that runs under your existing identity and permission system inherits your controls: who may do what, what is logged, where data stays. An agent hosted somewhere else needs those controls rebuilt, or goes without them.

Checklist

- Give each agent its own identity with the least access it needs. Never reuse a person's credentials.
- Log every tool call with who asked, what was called and what came back.
- Set limits on spend, time and number of steps, and decide what happens when a limit is hit.

- Know where prompts, outputs and any stored memory live, and how long they are kept.
- Treat a preview as a preview: plan for the interface to change before it is stable.

> Facts in this post were read from the sources listed below on 10 November 2026; this is a developing story or product and details may have changed since.

Sources and further reading

1. AWS News Blog. AWS Weekly Roundup: Amazon Bedrock Managed Agents powered by OpenAI, Q3 service availability updates, Kiro workflows, and more. 5 October 2026. aws.amazon.com/blogs/aws/aws-weekly-roundup-amazon-bedrock-managed-agents-powered-by-openai-q3-service-availability-updates-kiro-workflows-and-more-october-5-2026/
2. AWS News Blog. AWS Weekly Roundup: AgentCore Runtime V2, Amazon DynamoDB bulk put items, and more. 9 November 2026. aws.amazon.com/blogs/aws/aws-weekly-roundup-agentcore-runtime-v2-amazon-dynamodb-bulk-put-items-and-more-november-9-2026/

Published by IICTP, an independent technical credential body, on 10 November 2026. The current version of this post is at https://blogs.iictp.org/running-agents-under-existing-governance-bedrock-agentcore. More guides: blogs.iictp.org.