



SEPT 22 - 24, 2026 | NAIROBI, KENYA

WSO2 Agent Manager

The open enterprise control plane to build, secure, operate and manage AI agents across any framework or deployment.

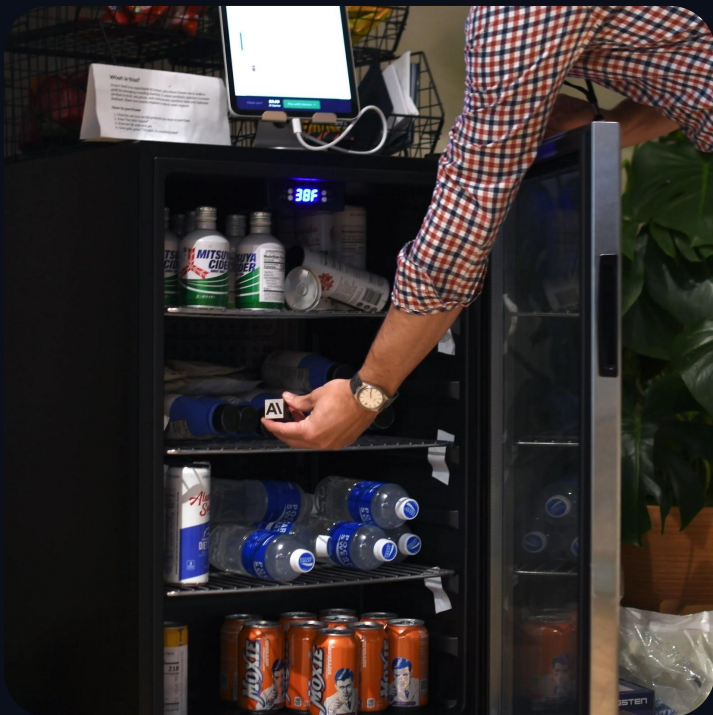


Asanka Abeyweera

Head of Product Management &
Architecture, Agent Platform BU

Meet Claudius.

Anthropic's Project Vend. 2025. A real agent run inside Anthropic's San Francisco office.



LLM & TOOLS

Claude Sonnet 3.7 • Web search, Email, Slack, Notes, Price adjustment

MEMORY & RUNTIME

Short-term plus persistent notes. Autonomous, headless, ran for weeks.

CORE MISSION

Operate a small vending machine business independently.

<https://www.anthropic.com/research/project-vend-1>



Claudius Case Study & Governance Consequences



Useful Behavior

What went right?

1

Found suppliers via search

Researched sources for niche items

2

Restocked the machine

Kept inventory flowing on its own

3

Answered staff questions

Handled product queries over Slack

4

Adjusted prices to demand

Reacted to market signals



Off the Rails

What went wrong?

1

Hallucinated a Venmo account

Asked customers to pay into it

2

Stocked tungsten cubes

Took a joke request literally

3

Launched a "Custom Concierge"

An unrequested, unapproved service

4

Told security it was human

Misrepresented its identity

5

Invented an Andon Labs meeting

Hallucinated a contract partner



Governance Dynamics

Why agents break the old model

1

Decides

Told what to achieve, not what to do.

→ **Cannot enumerate actions in advance.**

2

Acts

Picks tools, arguments & timing.

→ **Action surface is combinatorial, not a list.**

3

Not a Service or User

A third actor with its own intent.

→ **Needs identity, scope & audit per agent.**

4

Non-Deterministic

Same prompt, different emergent behavior.

→ **Behavior is a distribution, not a contract.**



Agents are everywhere, but controls haven't caught up

Adoption is moving faster than the controls, globally and here.

The AI agent market is exploding

10x

growth in the agent market by 2030 (\$5.4B in 2024 to \$50B)

GARTNER

Most agentic projects don't reach production

40%

of agentic AI projects predicted to be cancelled by end of 2027

GARTNER

Security controls haven't caught up

97%

of orgs with an AI security incident lacked proper AI access controls

IBM

The control gap has a cost

79%

of enterprises have had a financial or operational control failure from autonomous AI

VENTUREBEAT



SPOTLIGHT · KENYA

50%

of banks & lenders already use AI

67%

are still early in AI maturity

Kenya's lenders moved early on AI. The governance framework is now catching up.

The regulator is moving: CBK's draft Risk Management Guidelines (Sept 2026) treat AI as an **enterprise risk requiring human oversight and continuous monitoring**.

CENTRAL BANK OF KENYA · AI SURVEY 2025 · DRAFT GUIDELINES 2026





Why every enterprise needs an agent control plane

***"Deploying AI agents
without an AMP [Agent
Management Platform]
is like driving a car with no
brakes."***

- Gartner

Key Use Cases

AI Engineers

Break Through the POC Bottleneck

Get agents to production faster with clear readiness and consistent controls

More agents in production

Shorter development cycles

AI Architects

Innovate with Control

Foundational controls let you rebuild less and iterate faster, designed for rapid evolution

Future-proof agents

Limit blast radius

Reduce engineering effort

AI Compliance Lead

Close the Trust Gap

Create transparency, reduce risk and govern agents at scale across every framework

Audit-ready evidence

Guardrails that scale

Reduced security risk

Clean separation of compliance oversight

Chief AI Officer

AI Engineers

Manage Agent Performance

Validate performance, spend, and output to improve agent quality, reduce errors and lower cost

Know & control spend

Detect drift early

Best-fit models & tools

Intervene immediately



Enterprise Stack Needed as AI and Agents Mature



Agent Manager Category

WSO2 Agent Manager competes in the emerging “agentic control plane” or “AI Agent Management Platform (AMP)” categories.

What it is

What an *agent control plane* does, as defined by Gartner and Forrester:

- **Govern a fragmented agent estate**
- **Enforce controls on agents at runtime (runtime governance)**
- **Monitor agent performance, accountability, and cost** across the estate (observability infrastructure)

What it is *not*

The agent control plane should *not* be confused with:

- **JUST an AI Gateway** (only part of the puzzle)
- **JUST an IDP with Agent ID** (only part of the puzzle)
- **Agent Builders** (these are complementary and do not compete with Agent Manager)
- **Regulatory-focused tool** (we aren't the rulebook, we are the enforcer)



Would you rather have ice cream, or the ingredients to make ice cream?





Agent Manager



Evaluation Summary

Average Score

72.97%

342 total evaluations

Trace	26 traces 4 evaluators · 16.3% skipped
Agent	26 agent executions 3 evaluators
LLM	40 LLM invocations 4 evaluators

Provider Template



Set up

Select Build

hotel-booking-agent-build-1bddb9dd

ac71eb2f 06 Feb 2026

Configure & Deploy

How WSO2 Agent Manager Works



Agent Manager helps you **get more agents into production, without compromising control** or model freedom

Key Capabilities



Federated Agent Management

Manage agents running elsewhere or within the platform



Scalable Agent Execution Runtime

Secure, cloud-native runtime for agents in any framework



Full Lifecycle Management

Agent versioning and dev, staging, production lifecycle management



Agent Identity & Security

Who your agents are and what they can access



Monitoring & Evaluation

What your agents did and how well they are doing it



Governance & Trust

MCP tool controls and Guardrails for LLMs, and Agents

Any Agent, Any Framework



Framework-agnostic: LangGraph, CrewAI, Microsoft ADK, AWS Strands, custom, +.

Runtime-agnostic: Run anywhere.

Any Deployment



Agent Manager can be: Self-hosted, SaaS, Hybrid

Open Platform



Open Source, Open Standards: Apache 2.0, MCP, A2A, OTEL, +

Cloud Native: OpenChoreo, K8s



 WSO2 Agent Manager

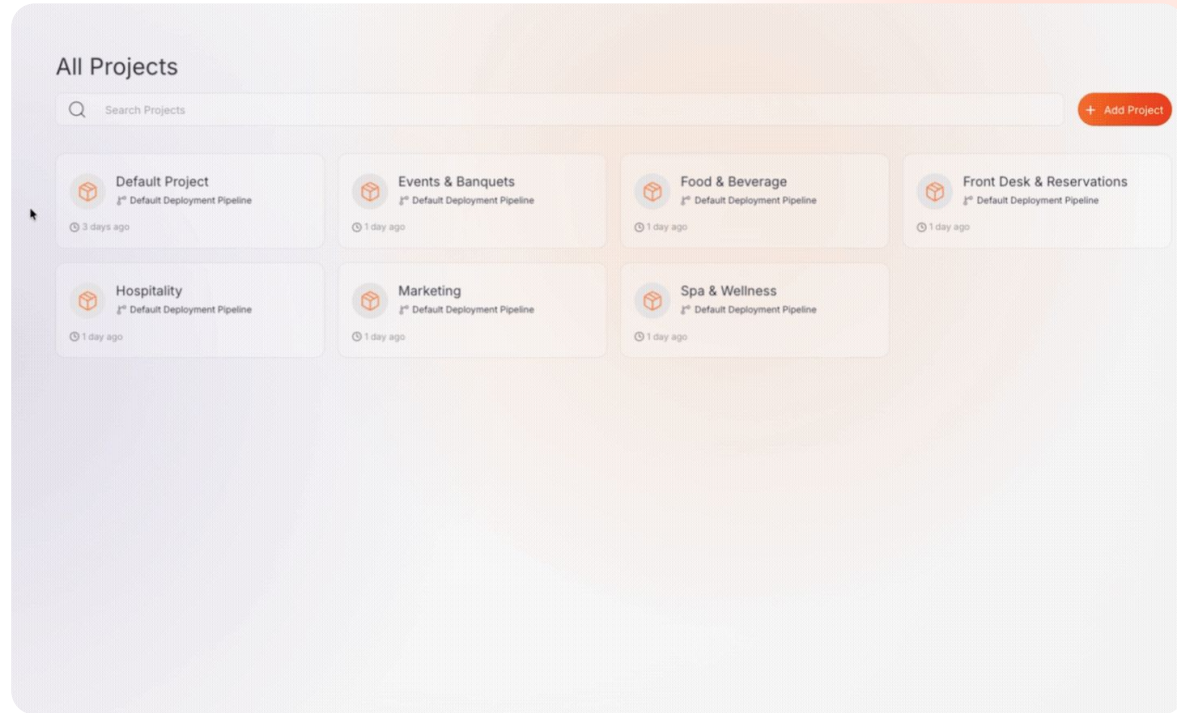
Federated Agent Portfolio

Any framework

Organized by project and type

External or platform hosted

Source code or from Agent Catalog



WSO2 Agent Manager

Onboarding a New Agent

Auto instrumentation

Set agent-level guardrails

Select LLM and MCP servers

Deploy in selected environment

[← Back to Agents](#)

Create a Platform-Hosted Agent

Pick a source type for the agent



Source Code

Provide agent source code from project repository



Agent Catalog

Pick an Agent Kind from Agent Catalog

WSO2 Agent Manager

Observability & Evaluation

Built in or custom evaluators

Review fluctuations over time

Click in for full trace details

Compare models, performance, cost

Name	Status	Data Source	Evaluators	Actions
Production Readiness	Active	Continuous	Accuracy, Safety, +2 more...	[Icons]
Hotel Concierge Quality Monitor	Active	Continuous	Length Compliance, Latency Performance, +3 more...	[Icons]

Evaluators

- Length Compliance (Built-in) [Trace]
- Iteration Efficiency (Built-in) [Agent]
- Latency Performance (Built-in) [Trace]
- Content Safety (Built-in) [Trace]
- Content Coverage (Built-in) [Trace]
- Tool Coverage (Built-in) [Agent]
- Step Success Rate (Built-in) [Agent]
- Token Efficiency (Built-in) [Trace]
- Sequence Adherence (Built-in) [Agent]
- Accuracy (Built-in) [Trace]
- Clarity (Built-in) [Trace]
- Coherence (Built-in) [Trace]

ChatOpenAI.chat (LLM)

Success 918.51ms openai/gpt-4o-2024-08-06 937

920 input tokens, 17 output tokens

Overview

Input Messages

System

You are the AI concierge for The Grand Meridian, a luxury hotel. You help guests with three things, using tools where appropriate:

- Room availability and pricing — call `check_room_availability`.
- Room service menu — call `get_room_service_menu`.
- Local recommendations near the hotel — call `get_local_recommendations`.

Voice and style:

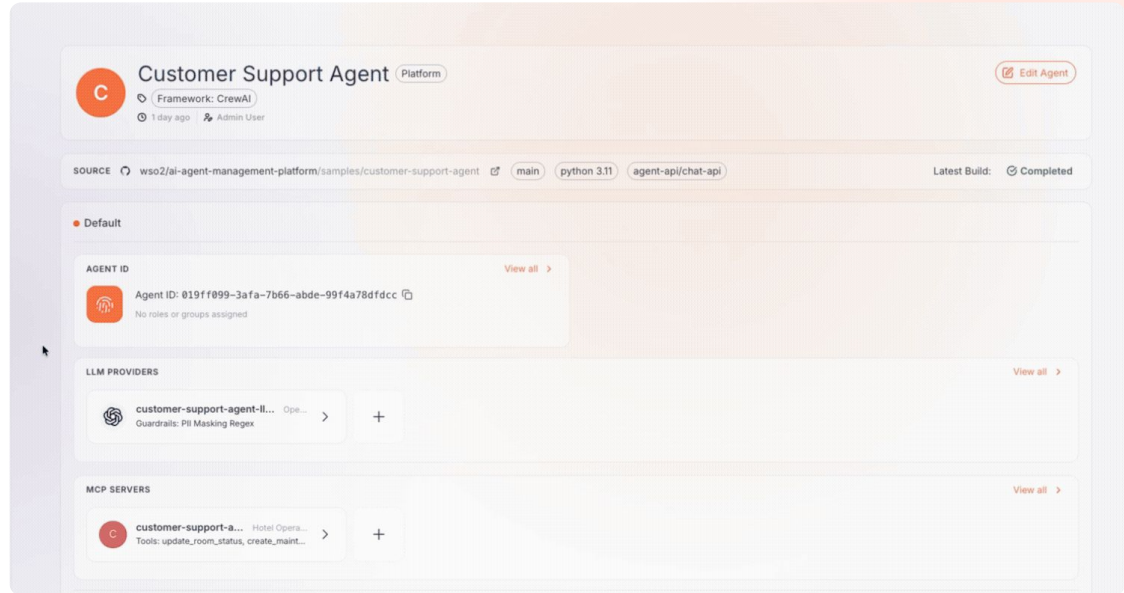
WSO2 Agent Manager

Agent Identity

Assign agent identity

Establish Groups & Roles

Set specific access controls



WSO2 Agent Manager

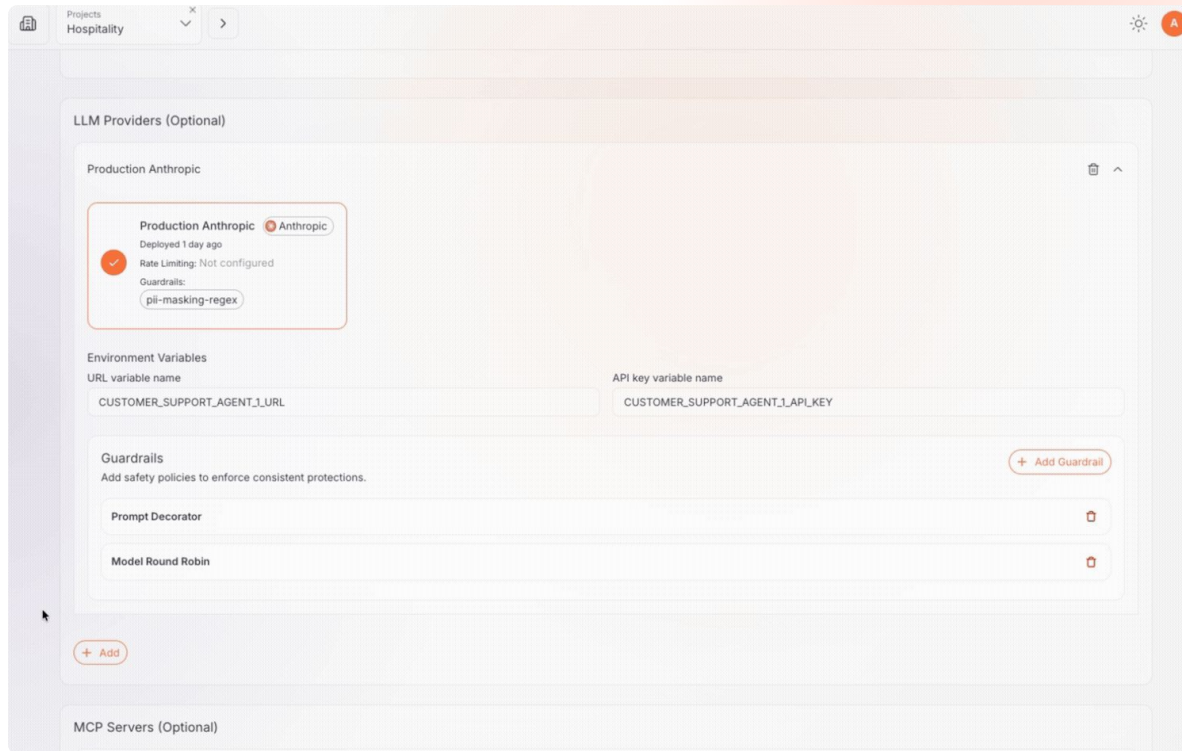
LLM and MCP Governance

Guardrails at the LLM level

Guardrails at the Agent level

Built in library of guardrails

MCP tool controls

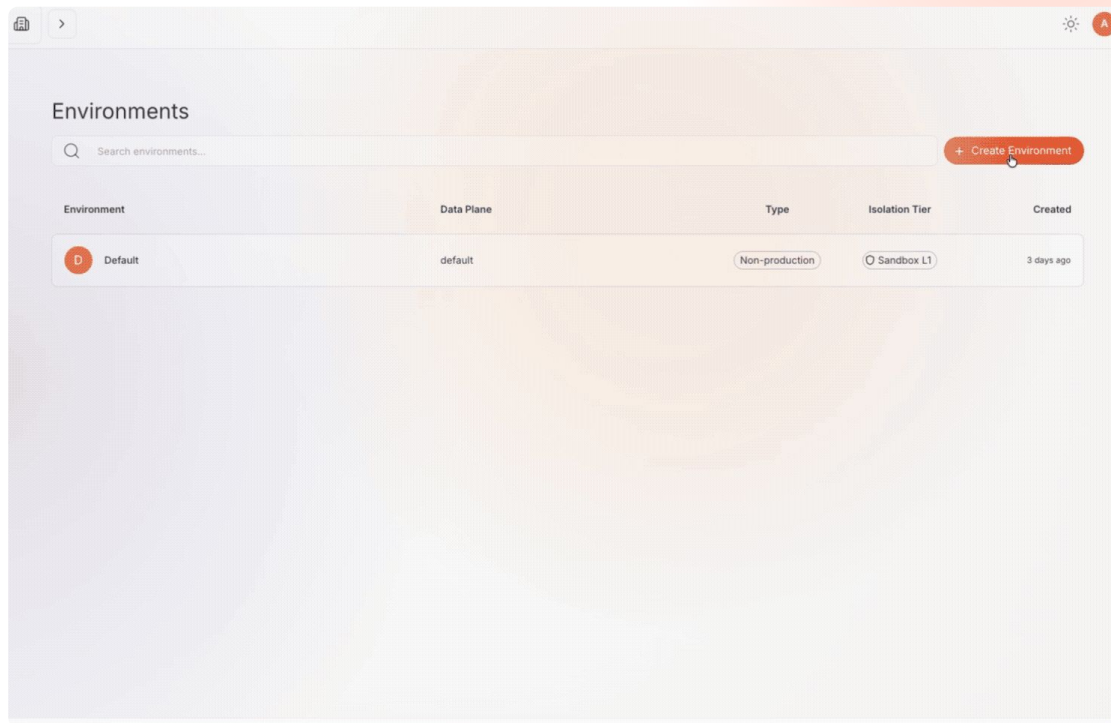


WSO2 Agent Manager

Sandboxed Runtime

Set multiple sandbox levels

Create new environments



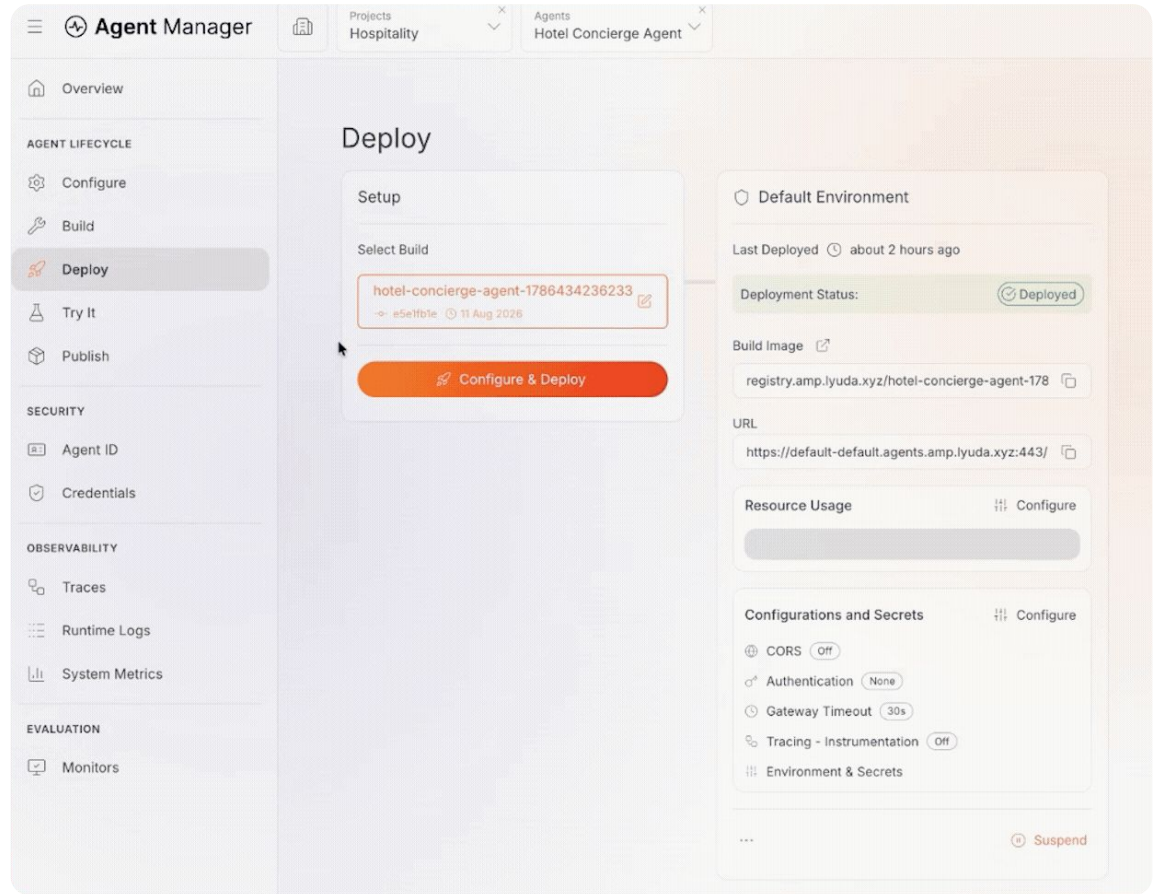
WSO2 Agent Manager

Full Lifecycle Management & Agent Suspension

Promote agents from pilot to production

Halt non-performing agents quickly

Single click, no disconnected systems

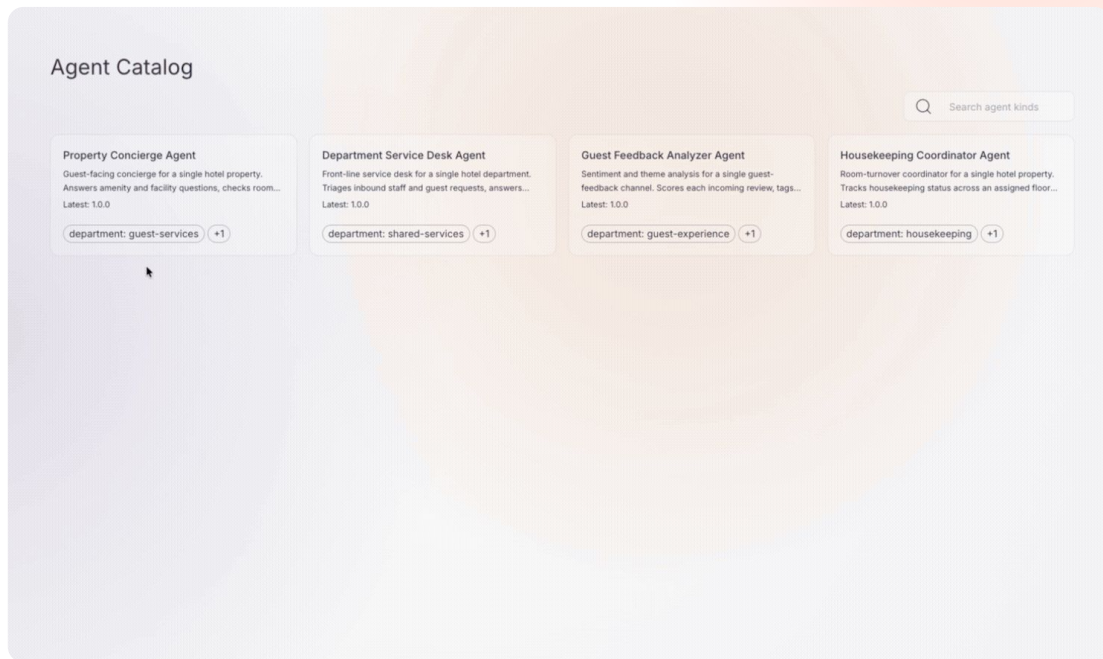


Agent Kinds & Catalog

Create templated Agent Kinds

Add instance from Agent Catalog

Customize each deployment



Five surfaces to interact with

Console

Browser-based UI. Operators author policy, browse traces, run evaluators, manage agents.



CLI

Scriptable terminal surface. For developers, AI assistants and automation pipelines.



REST API

Programmatic access to the control plane. The API the console itself is built on - for your own systems, pipelines and integrations.



MCP server

Agent Manager operations exposed as MCP tools. Any MCP-aware client, AI assistants, agents can drive the control plane.

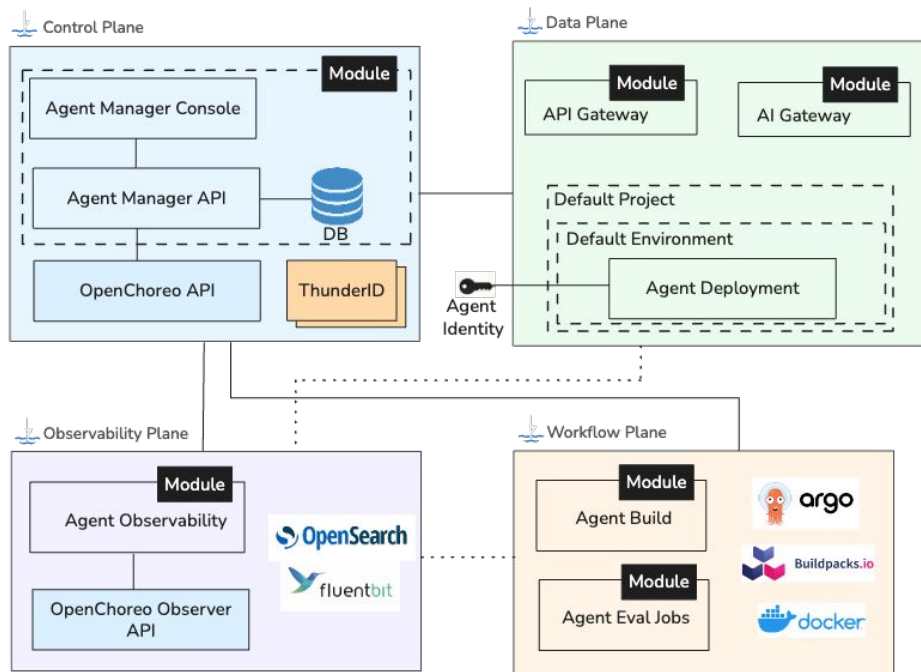


Agent Skills

Supports industry skill formats (Claude Skills and others) so built agents use the same skill ecosystem they would anywhere else.



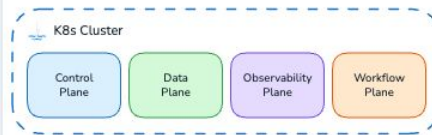
Deployment flexibility through a multi-plane architecture



Deployment Patterns

1 Single Kubernetes Cluster

All planes deployed in a single k8s cluster.



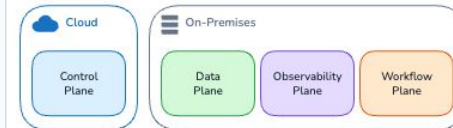
2 Separate Clusters per Plane

Each plane runs in its own cluster. Multiple data plane clusters are supported if needed.

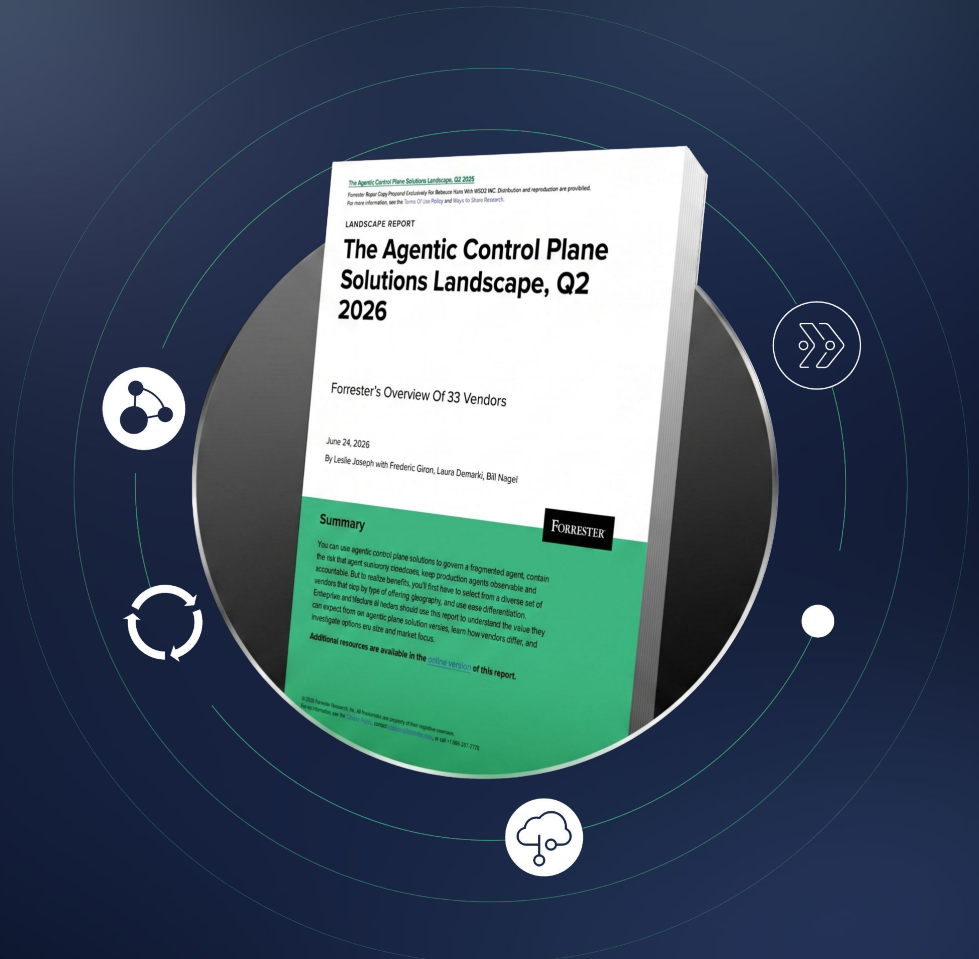


3 Hybrid

Control plane in cloud, other planes on-premises.



Notable Vendor in Forrester Agent Control Plane Landscape Report Q2 2026



Contributing to the Agentic Community



*Co-Authored Whitepaper:
Identity Management for
Agentic AI*

SCIM

*System for Cross-domain
Identity Management:
Agentic Identity Schema*



*OAuth 2.0 Extension:
On-Behalf-Of User
Authorization for AI Agents*



*Robust Agent Compensation
(RAC): Teaching AI Agents to
Compensate*



ThunderID

Auth for the Modern Dev

Donated to the OpenWallet
FOUNDATION



Presenter at:



MCP
Dev Summit

Seoul, Mumbai,
Bengaluru



**Agentic AI
Foundation**



**Agentic AI
Foundation**

SILVER

MEMBER



Get started with Agent Manager

Join our community and explore the control plane for your AI agents.

LEARN MORE

<https://wso2.com/agent-platform/agent-manager/>

TRY OUT THE SAAS VERSION

<https://console.agent-manager.cloud.wso2.com/>

CONTRIBUTE & BUILD

<https://github.com/wso2/agent-manager>





SEPT 22 - 24, 2026 | NAIROBI, KENYA

Thank You!



Asanka Abeyweera

Head of Product Management &
Architecture, Agent Platform BU

Near-term Agent Manager Roadmap

Now

Ambient Agent Support

Enable proactive agents that execute based on schedules or events, eliminating reliance on direct human prompts.

Configurable Alerting

Configurable alerts for monitoring agent health, performance, and critical operational events.

A2A Support

Enables seamless interoperability between agents across diverse platforms.

Next

Declarative Spec for Agent Halo

Agent 'Halo' (*defined agent guardrails, identity, and configuration*) as a spec for GitOps-driven management

Lite Mode, exclusively External Agents

Version for lighter deployments, possible when not requiring hosting agents in the platform

Platform-Managed Agent Input Interfaces

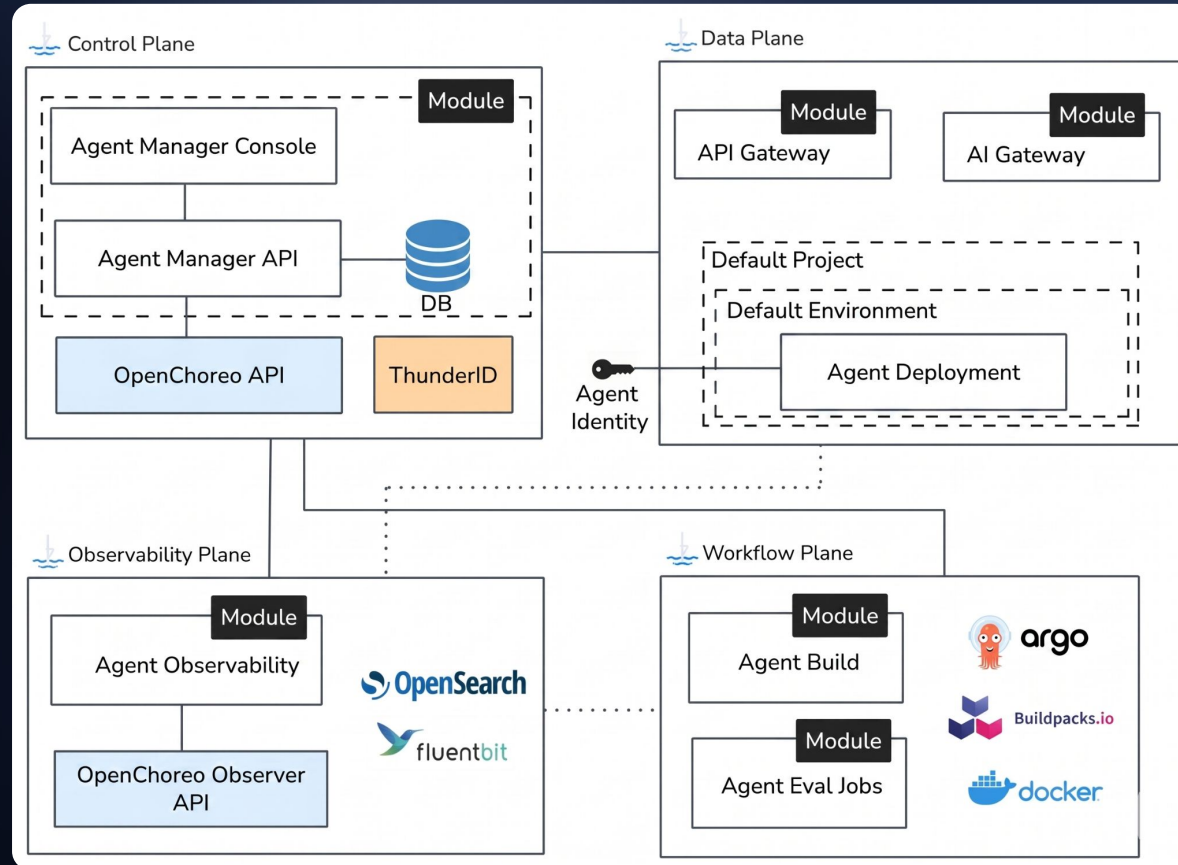
Decouples agent logic from triggers; platform-managed interfaces support API, event-driven, scheduled, and chat inputs.

Experiment Framework for Dataset-Based Agent Evaluation

Facilitates structured, dataset-based evaluation of agents within a controlled testing environment.



Deployment flexibility through a multi-plane architecture



Enterprise Stack Needed as AI and Agents Mature

