



# AI World

## Accelerating AI Agent Development with Oracle's Data Platform

---

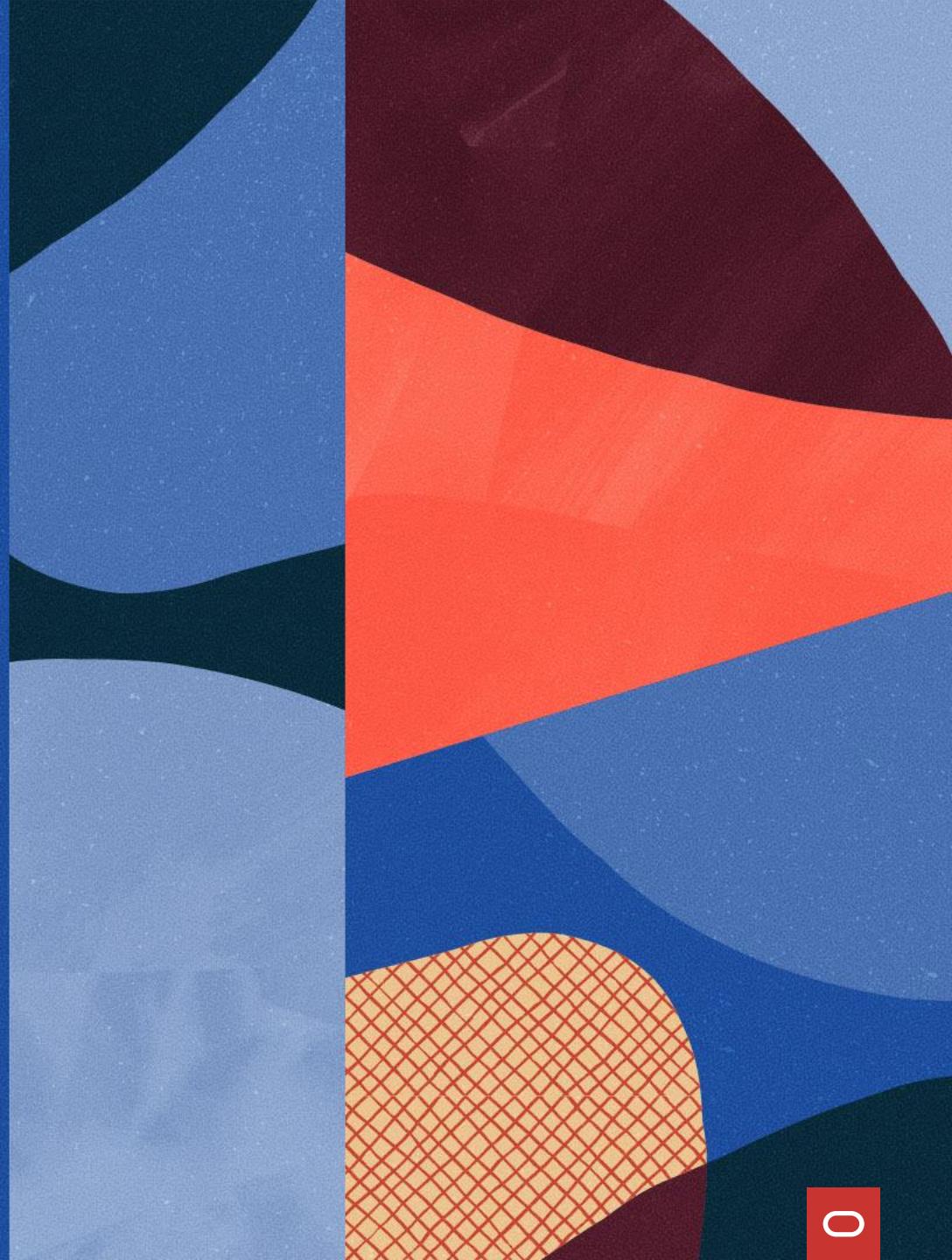
**Jean-Rene Gauthier**

Product Manager, Oracle AI Data Platform

**Colin Schmidt**

Vice President Engineering, Oracle AI Data Platform

October 15, 2025



## Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

# Speakers



**Jean-Rene Gauthier**

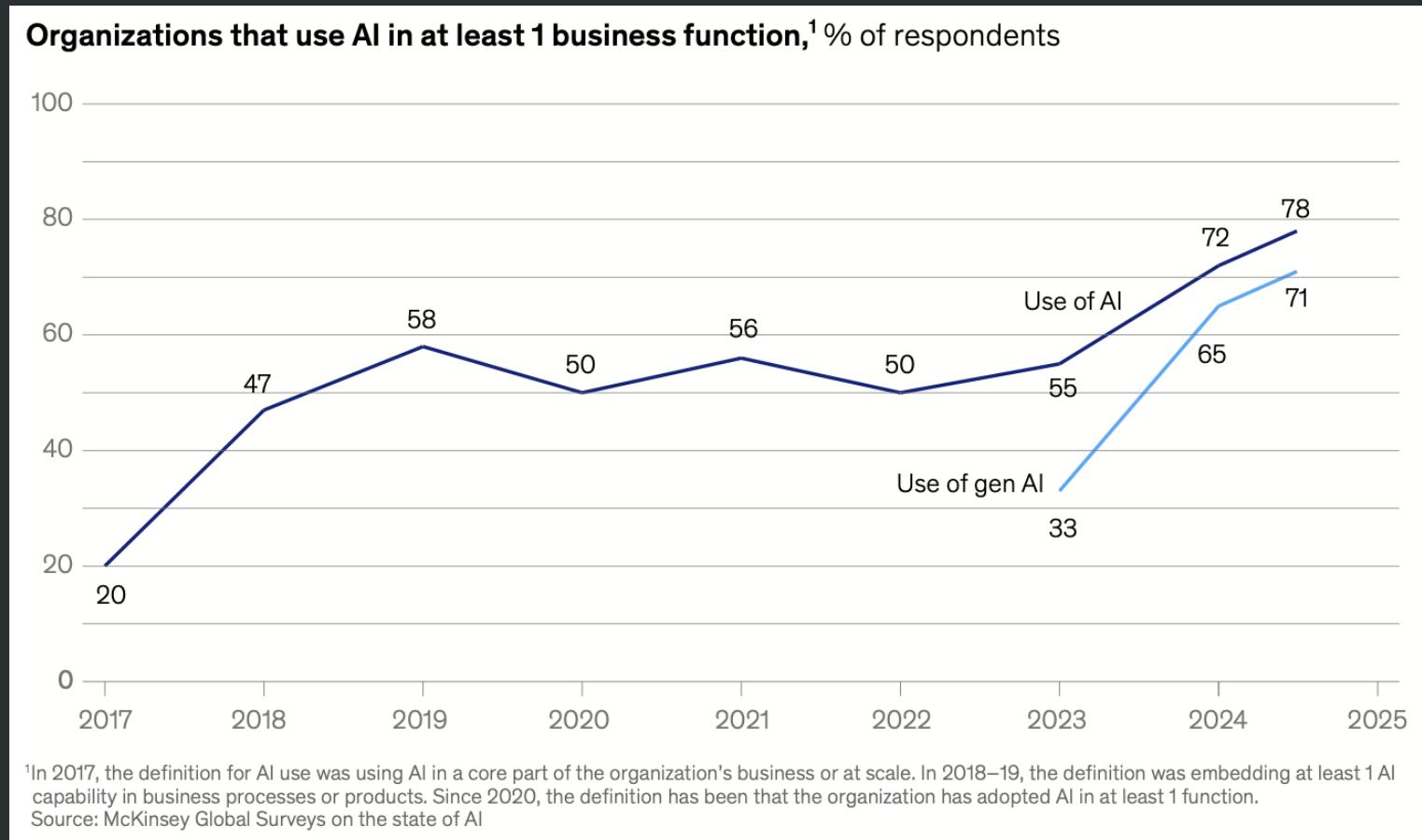
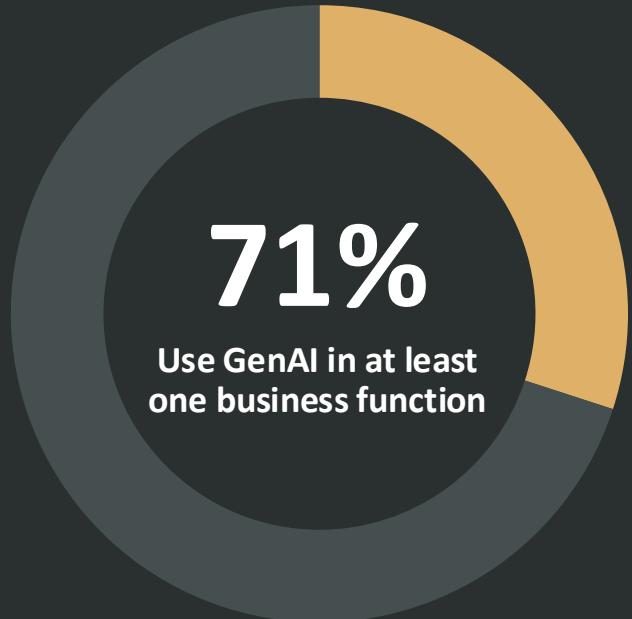
Product Manager, Oracle



**Colin Schmidt**

Vice President Engineering, Oracle

# GenAI adoption is climbing... and fast!



Source: McKinsey & Company, 2025

yet...

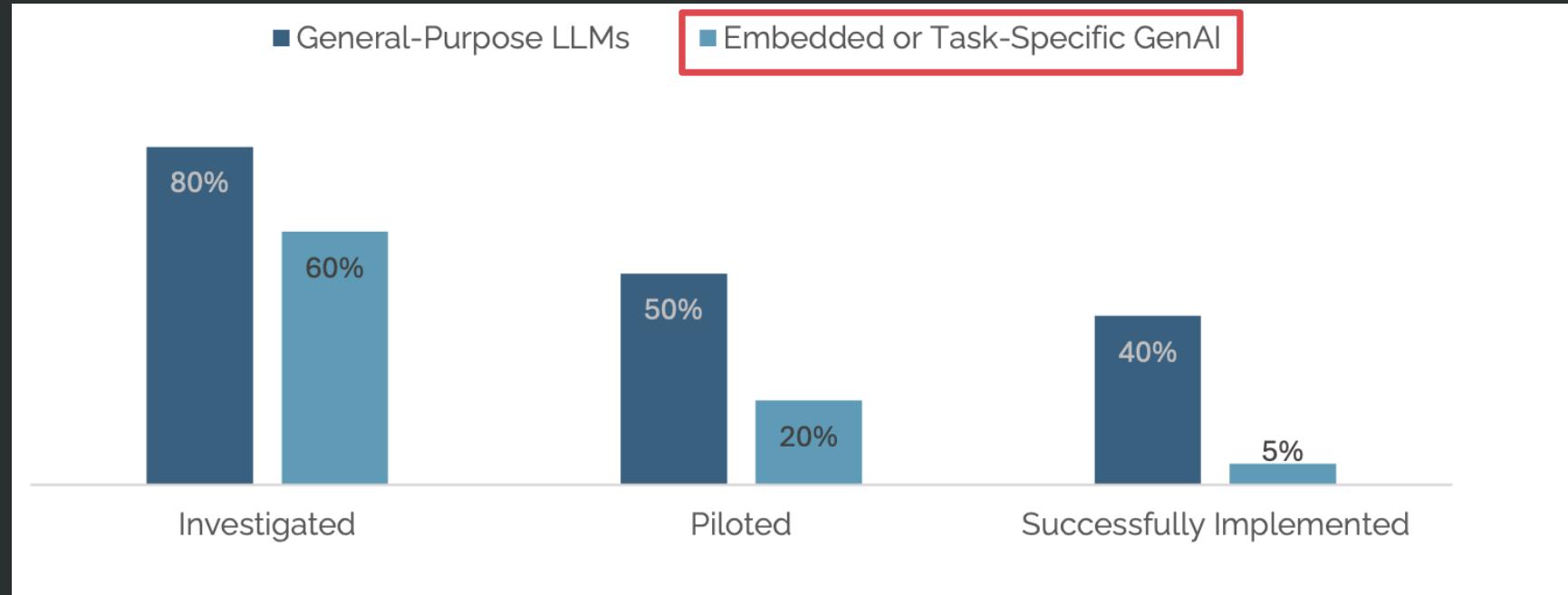
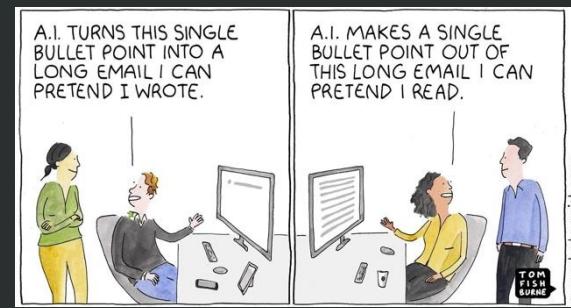
1%

---

of company executives describe their gen AI rollouts as mature

Source: McKinsey & Company, 2025

# But ChatGPT is great!

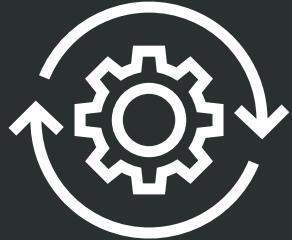


*For general purpose, adoption of GenAI through "unofficial channels" is very high... and successful!*

Source: MIT NANDA, 2025

# So why do task-specific AI agents fail?

Generic tools lack persistent memory and feedback loops



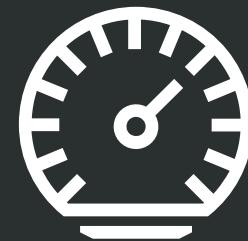
Agent needs deep customization aligned to internal data



Agent benchmarks need to be aligned with operational outcomes



Agents should be optimized for specific processes



Source: MIT NANDA, 2025

ANNOUNCING

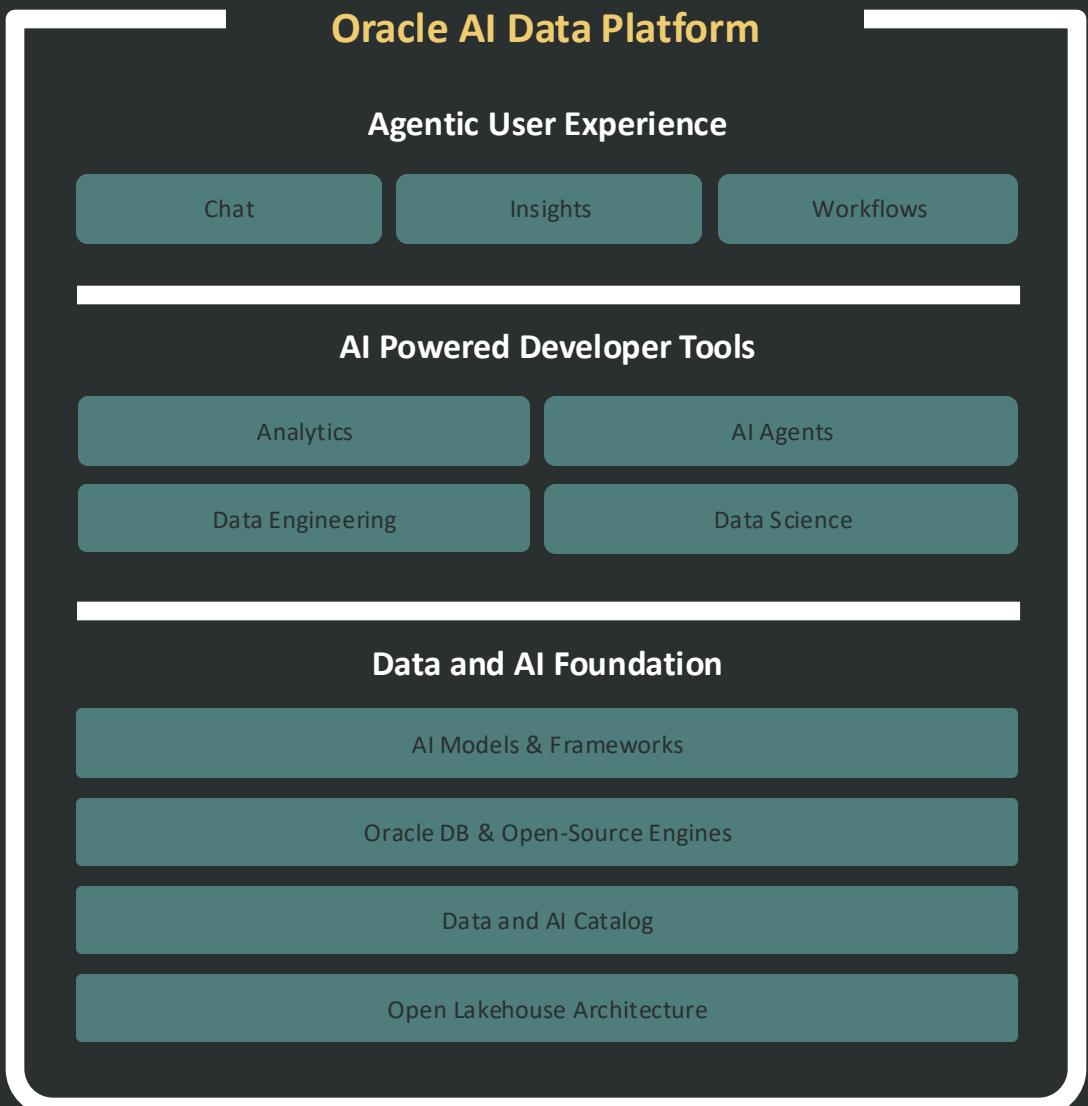
# Oracle AI Data Platform

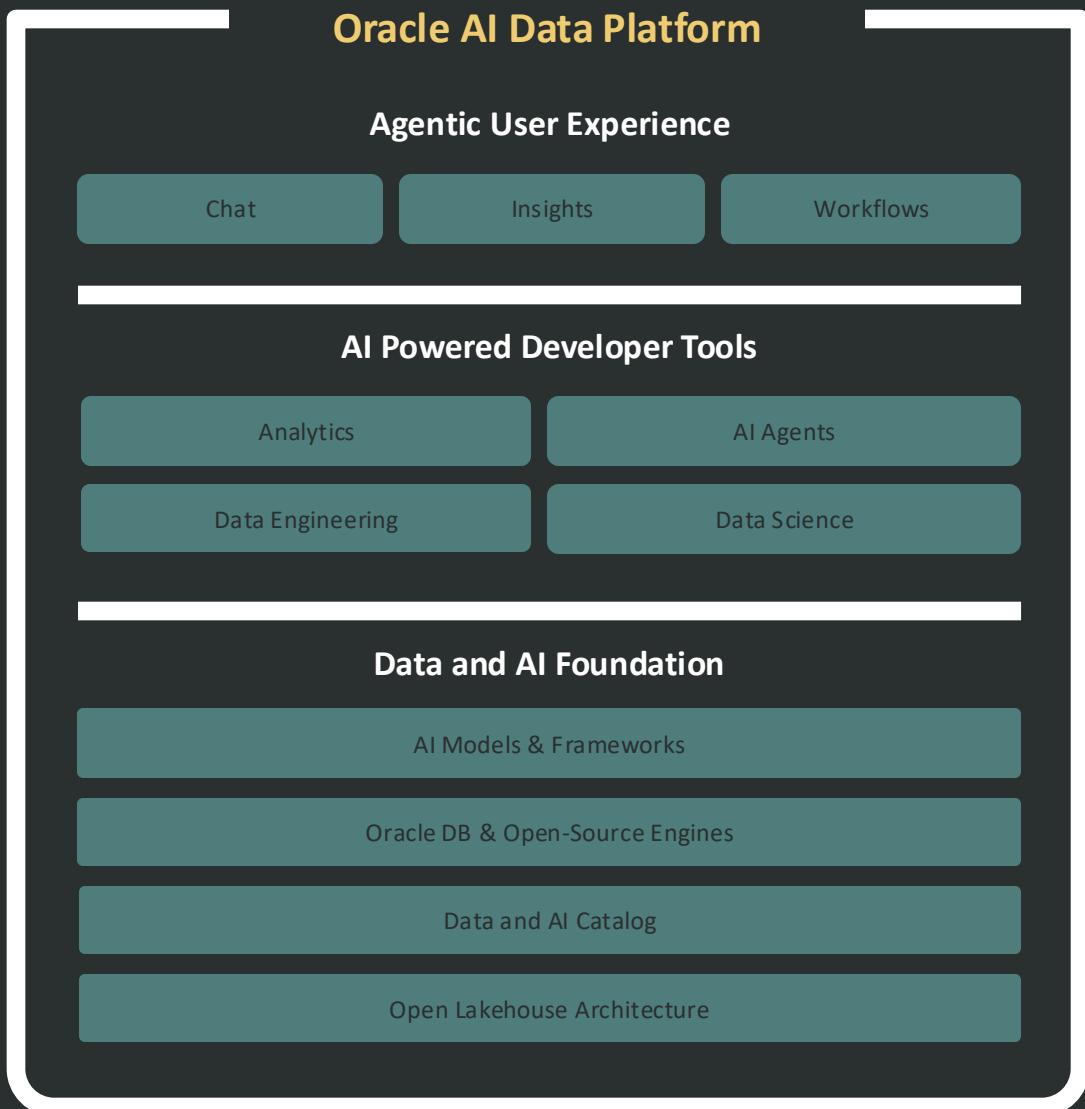
Empowering enterprises to build AI Agents and applications by uniting their enterprise data with best-in-class AI models and developer tools - driving innovation, efficiency, and competitive advantage.



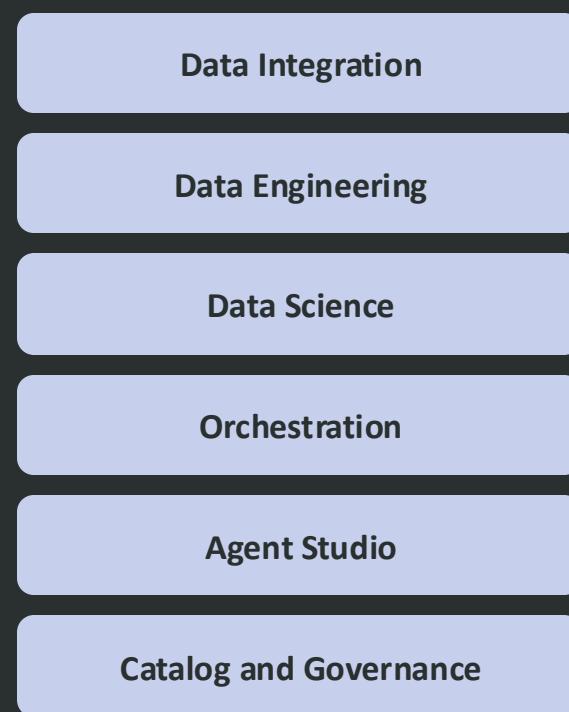
# Oracle AI Data Platform

Unified platform for lakehouse foundation, AI Agents, Tools, and business applications — built with enterprise-grade data and AI governance.





**Oracle AI  
Data Platform  
Workbench**





## Oracle AI Data Platform Workbench

Data Integration

Data Engineering

Data Science

Orchestration

Agent Studio

Catalog and Governance



Data  
Engineer



AI  
Developer



Data  
Steward



Data  
Scientist

AI Data Platform Workbench is a comprehensive developer environment for **data engineers, data scientists, developers, data stewards** to build and govern lakehouse foundations, AI applications and agents



# Data Platform

- **Multiple Data Integration Options**
  - Direct connectivity to multiple systems
  - Integrations with ADB, GoldenGate, MySQL Heatwave and OAC
  - FDI, EBS, Health
- **Unified Catalog, Governance, and Lineage**
  - Discover, organize, and govern all data and AI assets in a unified catalog across structured, semi-structured, and unstructured sources.
- **Support for Data Engineering and Data Science Workloads**
  - Notebooks, distributed processing, and model training on Spark clusters, unified workload management

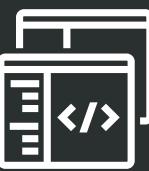
The screenshot shows the Oracle Data Platform interface with the 'Master Catalog' selected in the sidebar. The main pane displays a table of catalogs with columns for Catalog name, Catalog type, Source, Created on, and Created by. The table includes entries for Standard Catalogs (Default, Bronze, Silver, Gold, ADW, Auto Repair Catalog) and an External Catalog (FDI). The 'Created by' column shows 'System' or 'rohit.saha@oracle.com' for most entries, with 'rohit.saha' having three entries.

Catalog name	Catalog type	Source	Created on	Created by
Default	Standard Catalog	Intelligent Data Lake	Wed, May 22, 2023, 12:18:06 UTC	System
Bronze	Standard Catalog	Intelligent Data Lake	Wed, May 22, 2023, 12:18:06 UTC	rohit.saha@oracle.com
Silver	Standard Catalog	Intelligent Data Lake	Wed, May 22, 2023, 12:18:06 UTC	rohit.saha@oracle.com
Gold, ADW	Standard Catalog	Intelligent Data Lake	Wed, May 22, 2023, 12:18:06 UTC	rohit.saha@oracle.com
Auto Repair Catalog	Standard Catalog	Intelligent Data Lake	Wed, May 22, 2023, 12:18:06 UTC	rohit.saha@oracle.com
FDI	External Catalog	FDI	Wed, May 22, 2023, 12:18:06 UTC	rohit.saha@oracle.com

Demo: Master Catalog

# AI Agents in AI Data Platform





# AIDP Agent Development

- **Low-Code and Code-First AI Development**

Develop AI agents, tools, and applications using visual tools and/or notebook.

- **OCI Generative AI + Oracle 23ai Integration**

Leverage best-in-class LLMs and AI services.

- **Oracle 23ai Vector Store Integration**

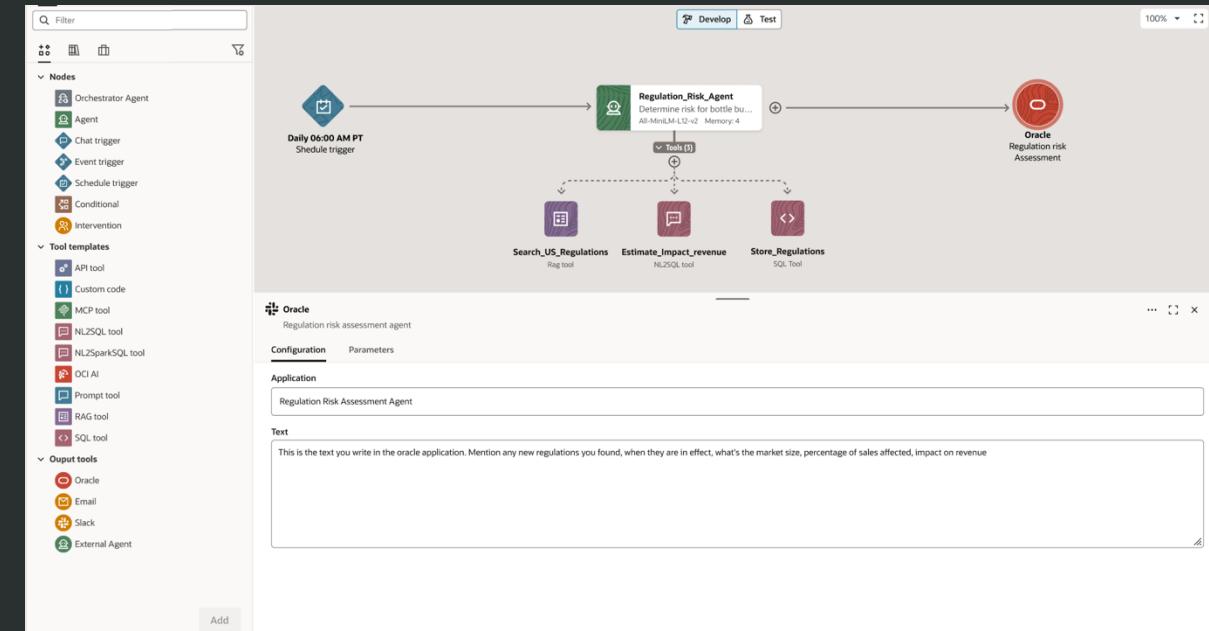
Store, manage, and query enterprise knowledge using vector search, linked to the master catalog.

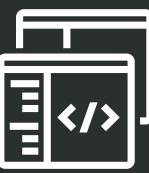
- **Lifecycle Management for AI Assets**

Register, version, test, and promote AI agents with full governance.

- **Fusion AI Agent Studio Integration**

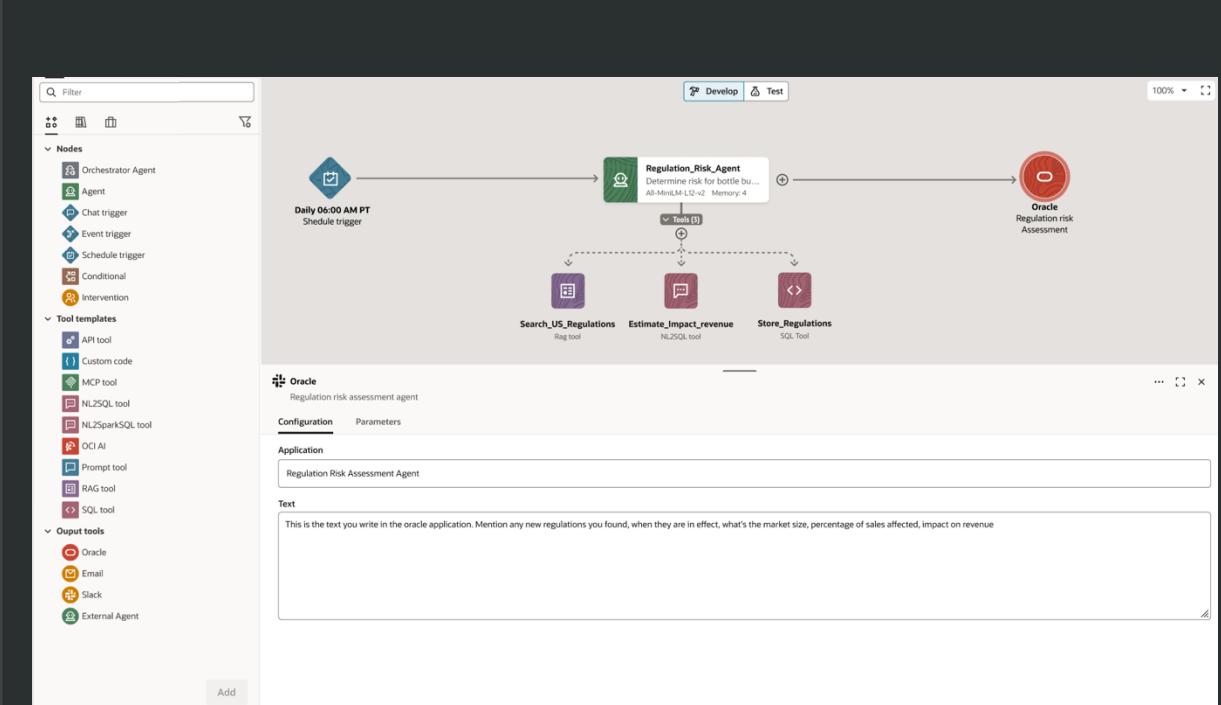
Embed custom agents directly into Oracle SaaS apps.

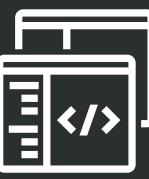




# Agent Flows

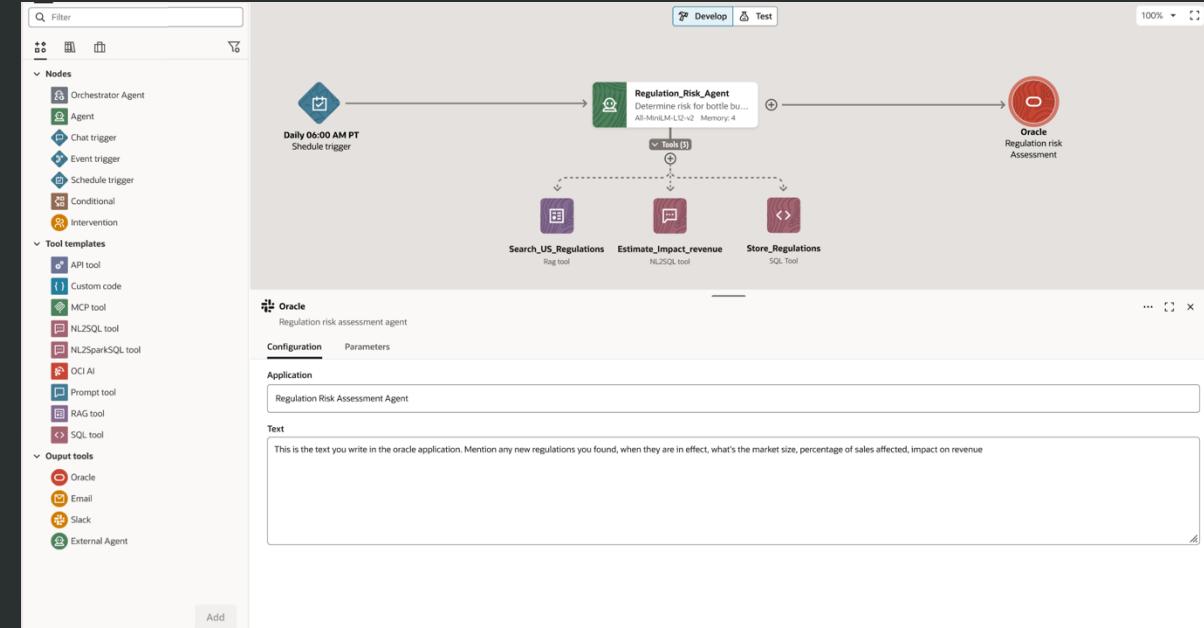
- Agent flows are E2E agentic applications that are core AI artifacts in AI Data Platform.
- Agent flows are defined through a graph of steps represented by nodes of different types (agents, tools, if/else condition, trigger, code, etc) and relationships
- Contrary to standard single- or multi-agent applications, agent flows let you orchestrate complex applications by mixing non-deterministic components (e.g. AI agents) with deterministic controls (e.g. triggers, code, conditional nodes)
- **Agent flows are designed to increase agentic applications reliability and predictability.**





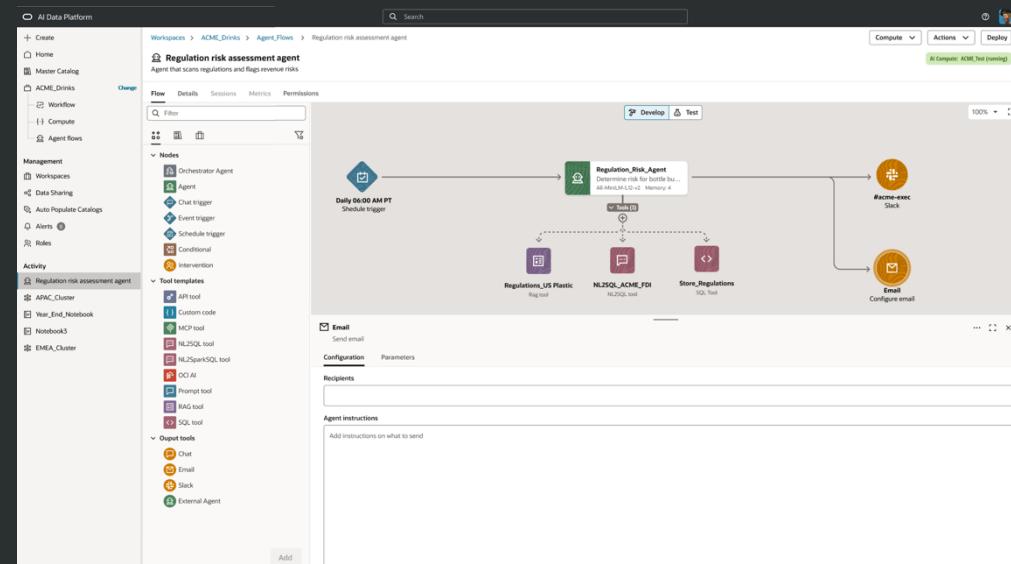
# Agent Flows

- Agent flows bring the best of agentic and Flexible application design which supports a variety of scenarios including:
  - Single agent with tools
  - Multi-agent systems
  - Partially deterministic execution through combinations of agent, code, trigger, and conditional nodes
- Supported node types include:
  - Trigger
    - chat, schedule-based, event-triggered, ad hoc
  - Conditional
    - If/else, branch split, etc
  - Code
    - custom code execution processing the output of another node
  - Agents
  - Tools

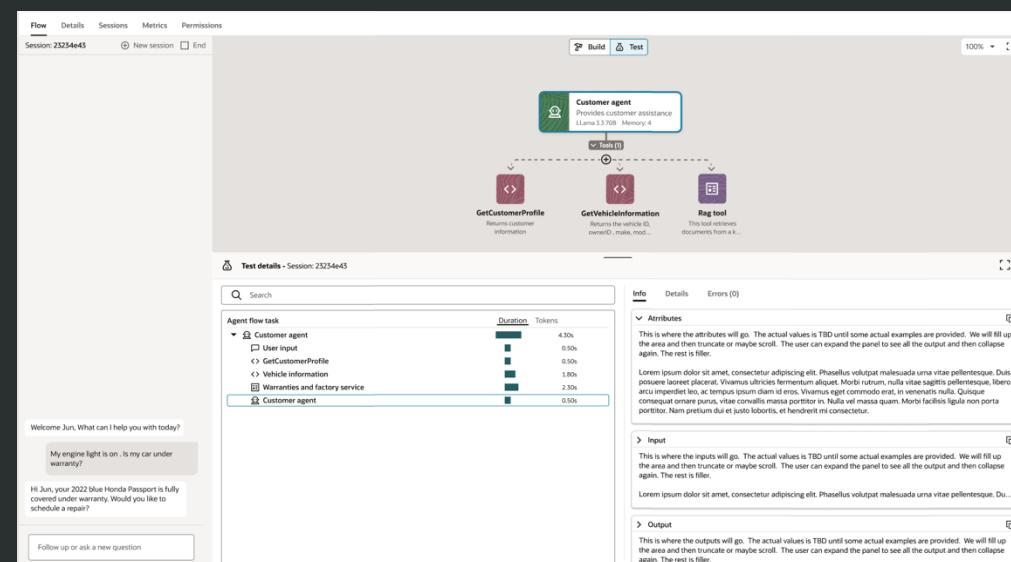


# Agent Flow Building, Testing, and Debugging

- Building agent flows is a highly iterative process.  
AIDP reduces the friction.
  - Support both no-code, canvas-style agent flow definition as well as code definition through LangGraph
  - Options to quickly iterate on your agent flow through “build” and “test” panels
  - Changes made to the agent flow in the “build” phase are immediately available for testing through a comprehensive testing playground.



Building



Testing

# Agent Flow Coding Experience



- Upload LangGraph app and/or author in AIDP Python editor
- Use AIDPUtils library to integrate Gen AI LLMs, Guardrails, Tools, Memory and Observability
- Define agent flow entry point file
- Configure a list of third-party Python dependencies
- Run and debug with a unified testing playground experience

The screenshot shows the AI Data Platform interface with the following details:

- Left Sidebar:** Shows navigation options like Create, Home, Master Catalog, WS\_DataEngineers (selected), Workflow, Compute, Agent Flows, Management, Workspaces, Data Sharing, Auto Populate Catalogs, Alerts, Roles, and Activity (AutoRepair\_Scheduling\_Agent selected).
- Center Panel:** Displays a tree view of workspace contents under WS\_DataEngineers > Agent\_Flows > AutoRepair\_Scheduling\_Agent. The tree includes Shared, Draft\_Notebooks, Agent\_Flows (with Sales\_Leads, Agent\_1, Agent\_2, Auto\_Repair), and AutoRepair\_Scheduling\_Agent (with .github, langgraph\_api, src/agent, static, test, tools, confless.py, .codespellignore, env, .gitignore, langgraph.json, license, Makefile, pyproject.toml, and README.txt).
- Right Panel:** Shows the "Code editor" tab for the "confless.py" file. The code editor interface includes tabs for Code editor, Test, Details, Sessions, Metrics, and Permissions. It displays the content of the confless.py file and includes standard file operations like File, Edit, View, and Save.



## Powered by Frontier LLMs from OCI Gen AI Service

- Select SOTA LLMs from the OCI GenAI service in your agent flow definition
- Configure the model parameters and provide detailed prompts to the agent including the objective, tasks, role, and any other relevant instructions.
- Configure tools and give your agent flow access to your data in AI Data Platform

 strok

 cohere

 Gemini

 Llama

 OpenAI



## Configurable Tool Templates available Out of the Box

*Reduce variance and give your agent flows the skills to access your valuable data*



### SQL Tool

Parametrize custom SQL queries to let your agent flows access data in AIDP catalog schemas.



### Retrieval Augmented Generation Tool

Connect to knowledge bases and Search through files stored in AIDP volumes.



### Prompt Tool

Give your agent access to prompt templates for email, notification, document summarization, etc.



# Protect your Agent Flow with Strong, Configurable Guardrails

- Ensuring that the agent flow behave according to expectations is paramount to AIDP
- AIDP provides **strong, default guardrails** that protects your agent flows against toxic and malicious content.
- Guardrails can also be configured and include:
  - Strong content moderation across multiple categories of harmful content: Hate speech, Harassment, Violence, Sexual, Derogatory, Toxic
  - Prompt injection
  - Apply for each **user query and/or model response**
  - Control if/how PII data are displayed in the query or the response
- Control the action to take by selecting between blocking the content, informing the end user or masking the PII content

The screenshot shows the 'Customer Agent' configuration page with the 'Safety Guardrails' tab selected. The interface is divided into sections for Content moderation prevention, Prompt attacks prevention, and PII detection, each with a list of entity types and configuration options.

Entity Type	Action	Threshold (0-1)
Hate speech	Block	.5
Harassment	Block	.5
Violence	Block	.5
Sexual	Block	.5
Derogatory	Block	.5
Toxic	Block	.5

**Content moderation prevention:**

Entity Type	Action	Threshold (0-1)
Person name	Block	.5
Address	Block	.5
Age	Block	.5
Date or time	Block	.5
Social security number or taxpayer ID (US)	Block	.5
Email	Block	.5

**PII detection:**



# Monitor Everything

- **Capturing all interactions** between user, agent flows, tools, data, and LLMs is necessary for development and production
- **Sessions, traces, spans, logs, errors, and token count** data generated during tests are available directly in the developer experience.
- **Inspect traces, drill down on spans, and spot errors** during conversations without parsing through logs
- Access a series of **metrics** giving you a pulse on the operational performance of your agent flow
- Enable the inspection of production sessions, traces, and metrics

The screenshots illustrate the Oracle AIOps platform's monitoring and tracing capabilities:

**Top Screenshot (Sessions Tab):**

Session ID	Status	URI origin	Start time	Duration	Tokens
abc-123-def-456-ghi-7890	Succeeded	https://ipsemlorem/tdfd	Fri, Sep 27, 2024 at 08:48:15 UTC	18 sec	4
abc-123-def-456-ghi-7892	Succeeded	https://ipsemlorem/tdfd	Fri, Sep 27, 2024 at 08:48:15 UTC	11 sec	5
abc-123-def-456-ghi-7893	Succeeded	Test	Fri, Sep 27, 2024 at 08:48:15 UTC	14 sec	2
abc-123-def-456-ghi-7894	Failed	Test	Fri, Sep 27, 2024 at 08:48:15 UTC	3.2 sec	7

**Bottom Screenshot (Details Tab):**

Session details - Session: 23234e43

Agent flow task	Duration	Tokens
Customer agent	4.50s	
User input	0.50s	
GetCustomerProfile	0.50s	
Vehicle information	1.80s	
Warranties and factory service	2.30s	
Customer agent	0.50s	

Info Details Errors (0)

Parent Session ID	23234e43
Trace ID	34345454
Start time	Wed, May 22, 2025, 12:18:06 UTC
End time	Wed, May 22, 2025, 12:18:10 UTC
Execution duration	4.2s
Execution tokens	2
Agent URI	rohit.saha@oracle.com
Resource URI	Retrieve weather
Source system	Chat window

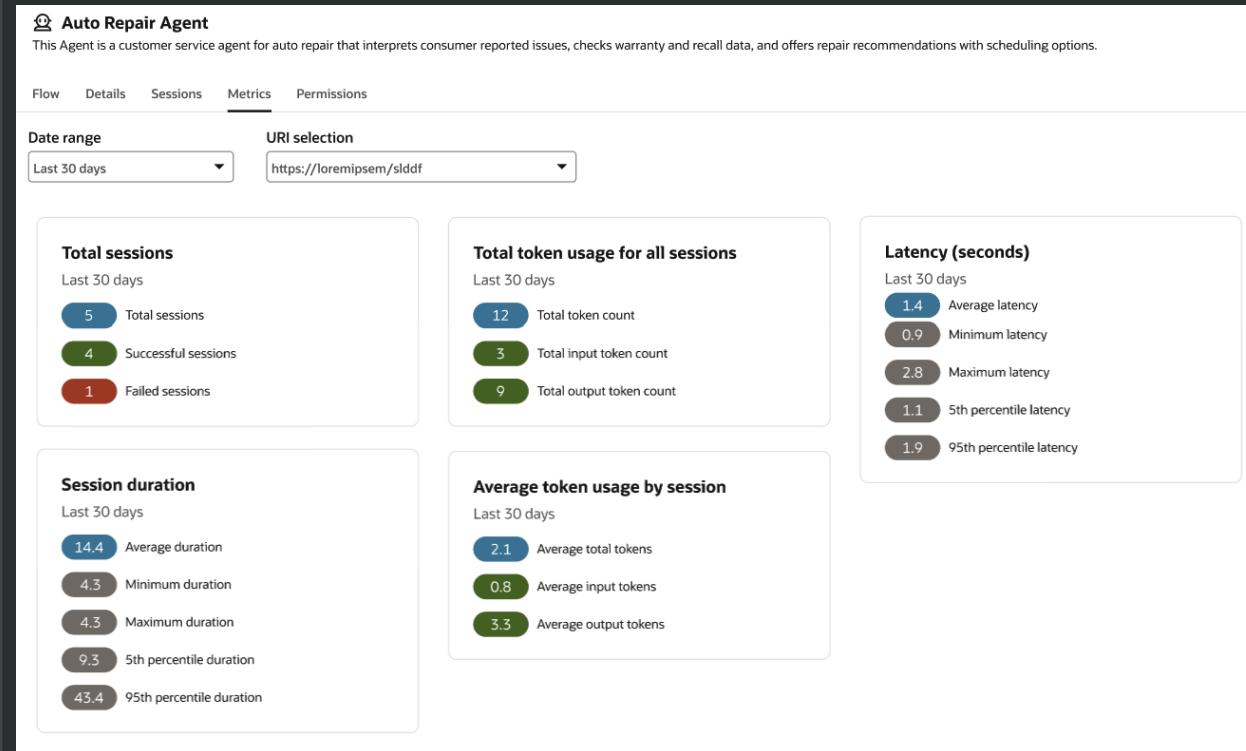
Chat history:

- Welcome Jun, What can I help you with today?
- My engine light is on . Is my car under warranty?
- Hi Jun, your 2022 blue Honda Passport is fully covered under warranty. Would you like to schedule a repair?



# Monitor Everything

- View operational metrics of your agent flow, including:
  - Session count
  - Session duration
  - Token consumption
  - Latency of each thread
- Select relevant time periods and inspect time series trends

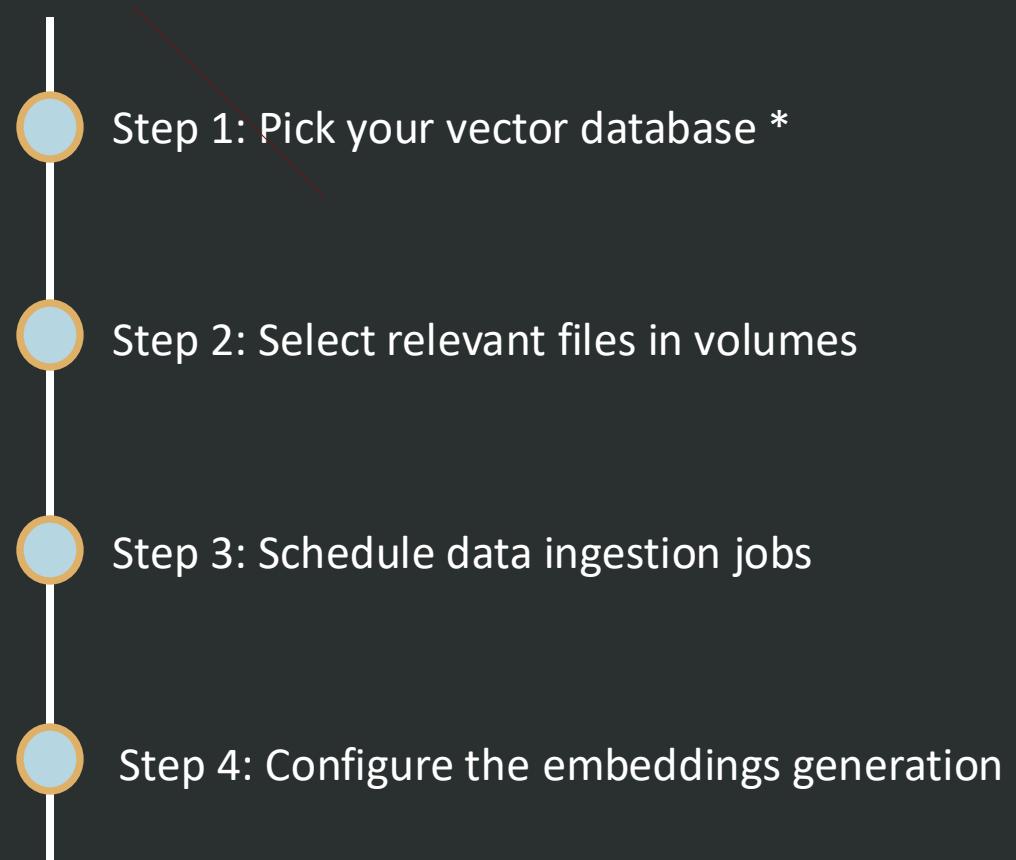


# Create Knowledge Bases in AI Data Platform

- Knowledge bases store vectorized representations of documents (pdfs, docx, html) stored in AI Data Platform volumes
- Agent flows can access knowledge bases to search and retrieve semantically relevant documents.



\* *all-MiniLM-L12-v2* and *multilingual-e5-small* are initially offered as embeddings models.



\* : or use the same ADW 23ai instance created during AIDP provisioning



# AI Data Platform Accelerates Agents Development



Unified data management, agent flow development, and deployment platform



Fast, no-code development experience or BYO code



Reduce time to value: tool templates to query your data



Agent protection through thoughtful default guardrails and unified RBAC



Leave no stone unturned and monitor everything

# Demo

---

The screenshot displays the Oracle AI Data Platform interface. On the left, the sidebar includes options like '+ Create', 'Home', 'Master Catalog' (which is selected), 'ACME\_Drinks', 'Management', 'Workspaces', 'Data Sharing', 'Auto Populate Catalogs', 'Alerts (8)', 'Roles', 'Activity', 'OCW\_Demo\_Notebook', 'APAC\_Cluster', 'Year\_End\_Notebook', 'Notebook3', and 'EMEA\_Cluster'. The main content area shows the 'Plastics\_Regulations' knowledge base under 'Master Catalog > ACME > Schema > Knowledge Bases > Plastics\_Regulations'. It provides a summary: 'Knowledge base for Plastics regulations for drinks'. Below this are tabs for 'Data Source', 'Details', 'Permissions', and 'History'. A table lists three data sources:

	Name	Type	Location	Ingest schedule	Added on	Added by
<input type="checkbox"/>	US	Table	ACME/Default_Schema/Tables/US_Regulations	Daily at 6am	Wed, May 22, 2023, 12:18:06 UTC	rohit.saha@oracle.com
<input type="checkbox"/>	EMEA	Bucket	International_Regulations/container/EMEA	Daily at 6am	Wed, May 22, 2023, 12:18:06 UTC	rohit.saha@oracle.com
<input type="checkbox"/>	APAC	Bucket	International_Regulations/container/APAC	Daily at 6am	Wed, May 22, 2023, 12:18:06 UTC	rohit.saha@oracle.com

# AI Data Platform Workbench | Roadmap Timeline



## Q3 2025 - General Availability

### Data and ML Developers

- Developer workspaces
- Notebooks & job orchestration
- Apache Spark – Python, SparkSQL
- Notebook Code Assist
- Orchestrate & monitor data pipelines
- Open-source libraries & frameworks
- Compute – Intel, AMD, GPU
- Delta Share

### AI Developers

- OCI Gen AI models – Llama, Cohere, OpenAI

### Catalog and Governance

- Catalog for data and models
- Object store (Standard Catalog)
- ADB, Exadata, Oracle DB (External Catalog)
- RBAC at table or column level

### Integrations

- ADB as a source and target
- OAC – Connect to AIDP Catalog
- FDI – share data/metadata
- Fusion – built-in connector

## Q4 2025

### AI Developers

- OCI Gen AI models – Llama, Cohere, OpenAI
- Tool Types – RAG, SQL, Vector, LLM
- Low-code agent flow creation
- Agent endpoint deployment
- Agent-flow testing playground
- Observability
- Guardrails

### Catalog and Governance

- AI knowledge support

### Integrations

- GoldenGate – AIDP lakehouse as Target

## 2026

### Data and ML Developers

- Iceberg support
- Scala
- MLOps
- GIT/CICD

### AI Developers

- Multi-Agent support
- MCP server for tools
- Fusion AI Agent Studio integration
- Custom Tools

### Catalog and Governance

- Lineage
- Data Quality

### Integrations

- 3P data stores, such Azure Blob



# Q&A

---

# Thank you

---

[jr.gauthier@oracle.com](mailto:jr.gauthier@oracle.com)

[colin.j.schmidt@oracle.com](mailto:colin.j.schmidt@oracle.com)

# Unlocking the Future: See How AI Is Transforming Analytic Applications

## Srikant Gokulnatha et al.

**Wed Oct 15, 2:15-3:00PM, Ballroom F, level 2**

### Data Engineering for AI Using Oracle AI Data Platform

Sujoy Chowdhury  
Martin Jung

Marco Polo 805, Level 1

**Wed Oct 15  
3:30-4:15pm**

### Learn How Partners Accelerate AI Innovation with Oracle AI Data Platform

Santosh Balasubramanian et al.

Titian 2205,  
Level 2

### AI Predictions with Medallion Architecture and LLMs on Oracle AI Data Platform (Lab)

Sujoy Chowdhury et al.

Expo 306,  
Level 1

### Building Agents with Oracle AI Data Platform: Best Practices

Guy Michaeli  
Katrín Kirchhoff  
Timothy Naxon

Marco Polo 803, Level 1

**Thu Oct 16  
11:30-12:15pm**

### From Data to Predictions: Building AI Models with Oracle AI Data Platform

Sujoy Chowdhury

Marco Polo 804, Level 1

**Thu Oct 16  
9:00-9:45am**

**Your feedback is important.**

**Scan this QR Code or use the  
Mobile App to share your  
thoughts on this session.**



ORACLE