ORACLE
AI World

Qualys.

Agentic AI on Vulnerability Management

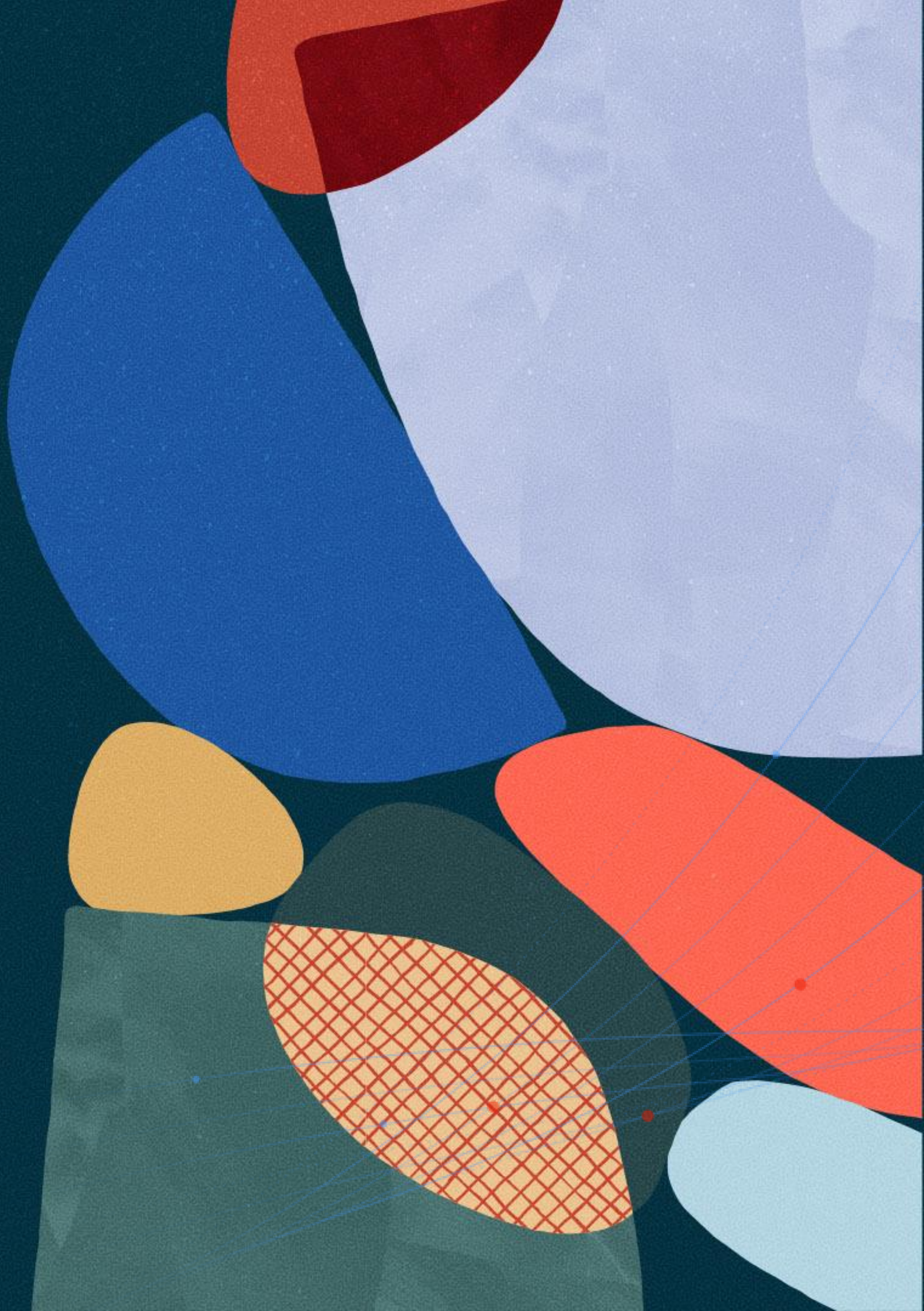
Transforming Cybersecurity from Reactive to Autonomous

Balaji Venkatesan

Senior Director AI and Data Platform

Saurabh Mishra

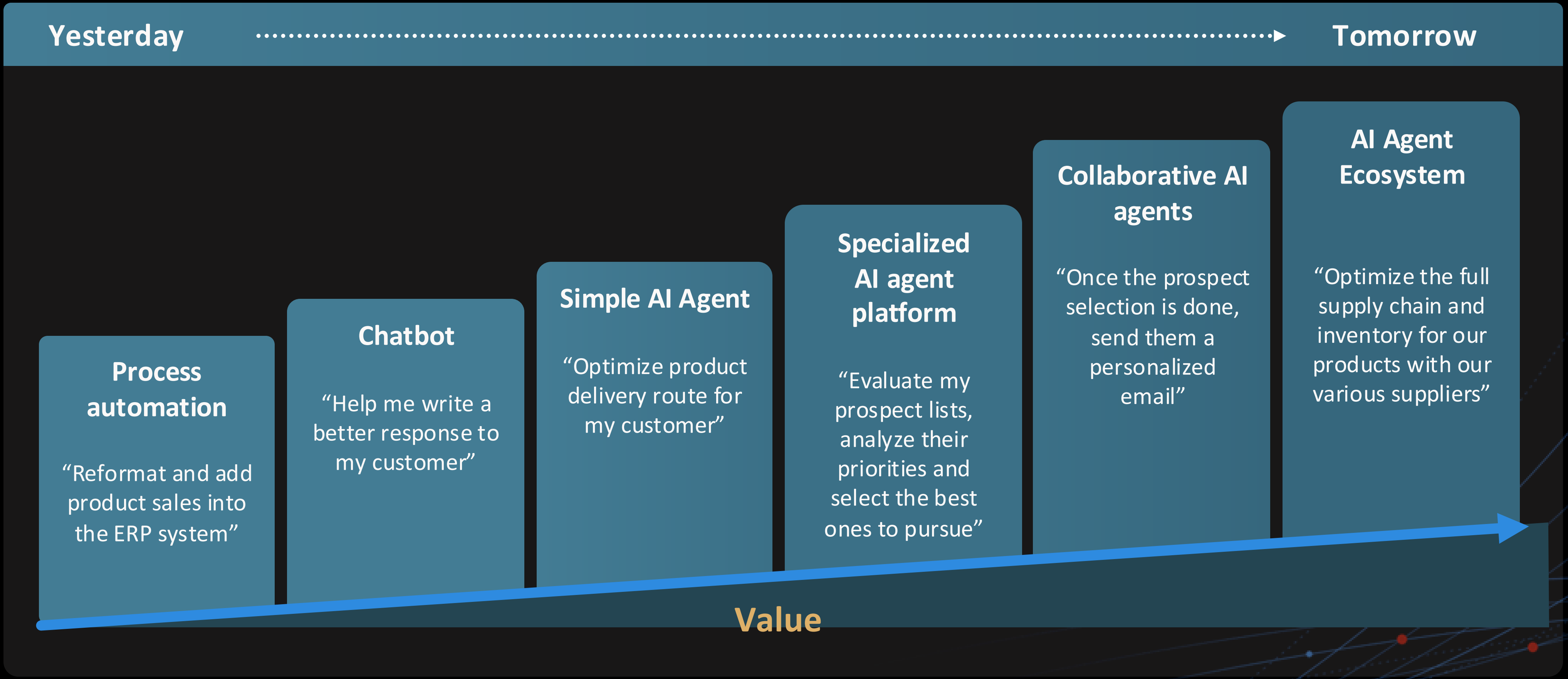
Field CTO – Oracle NA Specialists



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.

The shift from reactive AI models to autonomous, AI-driven agents is happening



Yesterday → Tomorrow

Process automation

"Reformat and add product sales into the ERP system"

Chatbot

"Help me write a better response to my customer"

Simple AI Agent

"Optimize product delivery route for my customer"

Specialized AI agent platform

"Evaluate my prospect lists, analyze their priorities and select the best ones to pursue"

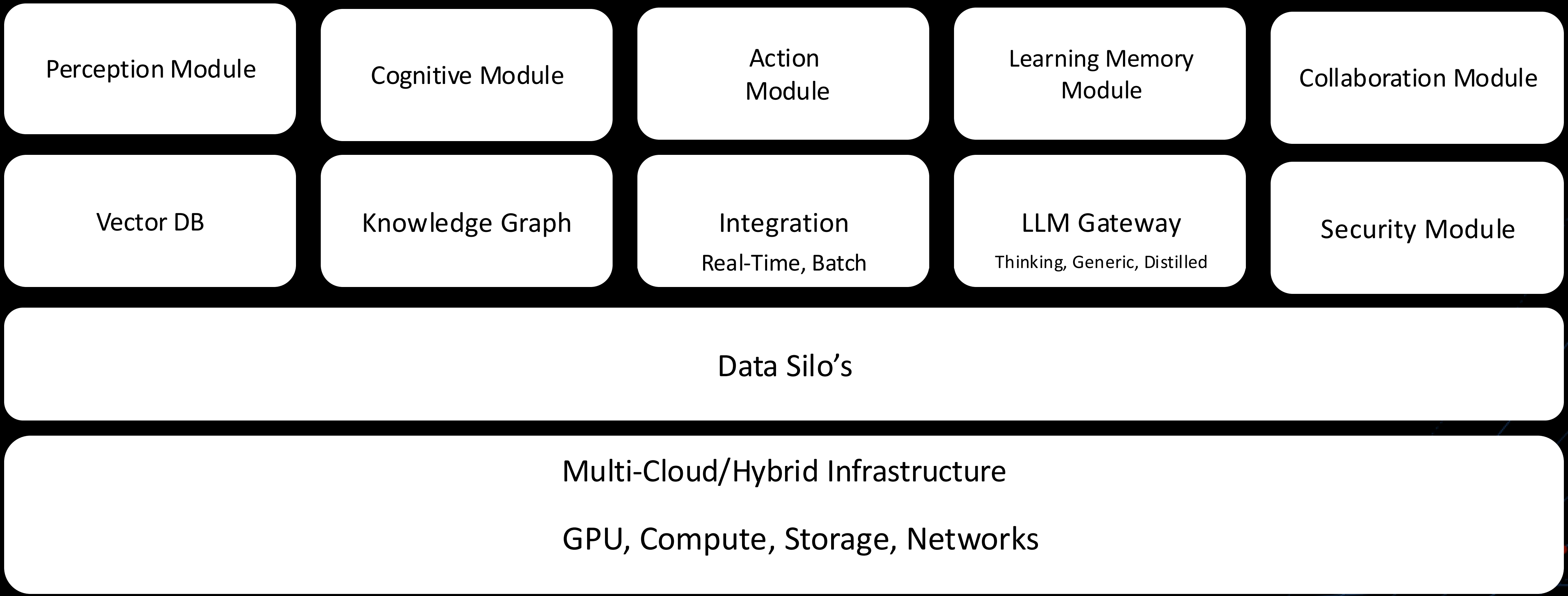
Collaborative AI agents

"Once the prospect selection is done, send them a personalized email"

AI Agent Ecosystem

"Optimize the full supply chain and inventory for our products with our various suppliers"

Enterprise Agentic AI Platform – Building Blocks



Perception Module

Cognitive Module

Action Module

Learning Memory Module

Collaboration Module

Vector DB

Knowledge Graph

Integration

Real-Time, Batch

LLM Gateway

Thinking, Generic, Distilled

Security Module

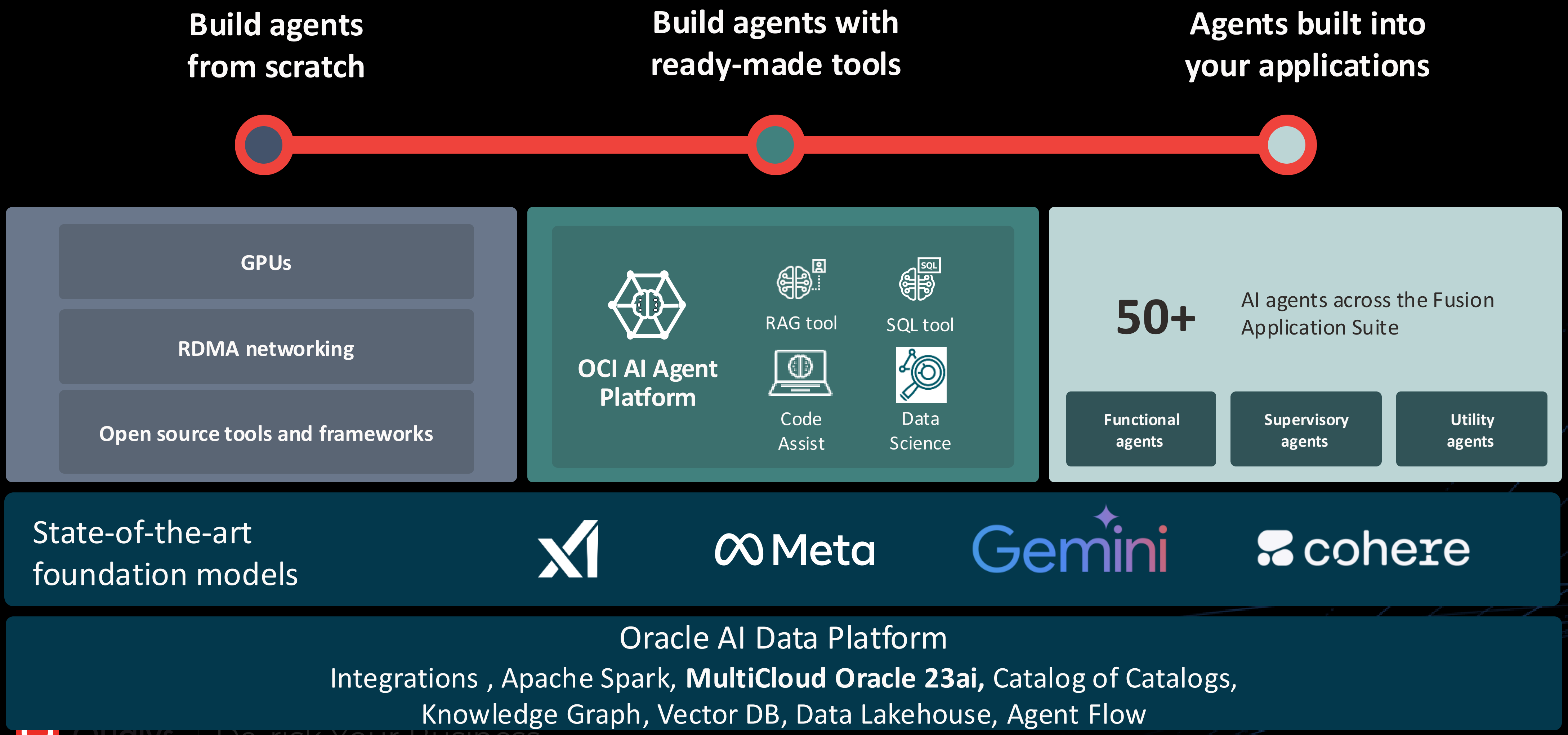
Data Silo’s

Multi-Cloud/Hybrid Infrastructure

GPU, Compute, Storage, Networks

Oracle provides choice

Agents how you want them, where you want them



Build agents from scratch

Build agents with ready-made tools

Agents built into your applications

GPUs

RDMA networking

Open source tools and frameworks

OCI AI Agent Platform

RAG tool

SQL tool

Code Assist

Data Science

50+ AI agents across the Fusion Application Suite

Functional agents

Supervisory agents

Utility agents

State-of-the-art foundation models

Oracle AI Data Platform

Integrations , Apache Spark, **MultiCloud Oracle 23ai,** Catalog of Catalogs, Knowledge Graph, Vector DB, Data Lakehouse, Agent Flow

Let's delve deeper…

Qualys.

Current Vulnerability Management Challenges

Median time for threat actors to weaponize vulnerabilities: 5.5 days

Security teams overwhelmed by tool sprawl and disconnected findings

Average organization unaware of up to 25% of internet-facing assets

30% of cloud VMs running with high/critical vulnerabilities

5% of CISA KEVs remain unpatched for over 90 days

Manual workflows create reactive, time-consuming processes

What is Agentic AI?

AI systems designed to function as autonomous agents capable of planning, decision-making, and executing complex workflows with minimal human oversight

- Contextual awareness and multi-step reasoning
- Goal-driven behavior beyond reactive tasks
- Self-orchestrating capabilities at machine scale
- Autonomous identification, prioritization, and remediation

Qualys Agentic AI Solution

Two Main Innovations

Marketplace of Ready-to-use Cyber Risk AI Agents

Cyber Risk Assistant (prompt-driven interface)

Key Features

Integrated into Enterprise TruRisk Management (ETM)

Built on Qualys AI Fabric architecture

Enables autonomous cybersecurity operations

Three Foundational Capabilities

Natural Language Query (NLQ)

- Democratized access to complex security datasets
- Plain-language interface for technical and non-technical users

Intelligent Decision Support

- Self-learning analytical engine
- Contextual risk evaluation based on business impact

Autonomous Response

- Real-time threat detection and remediation
- Reduced Mean Time to Resolution/Remediation (MTTR)

Agentic AI Architecture Overview

Key Components

- Global MCP Server (entry point)
- Centralized Orchestrator/Coordinator Agent
- Planner/Router Agent
- Module-specific agents: MCP Server, Planner, Data, Action, Helper

Workflow

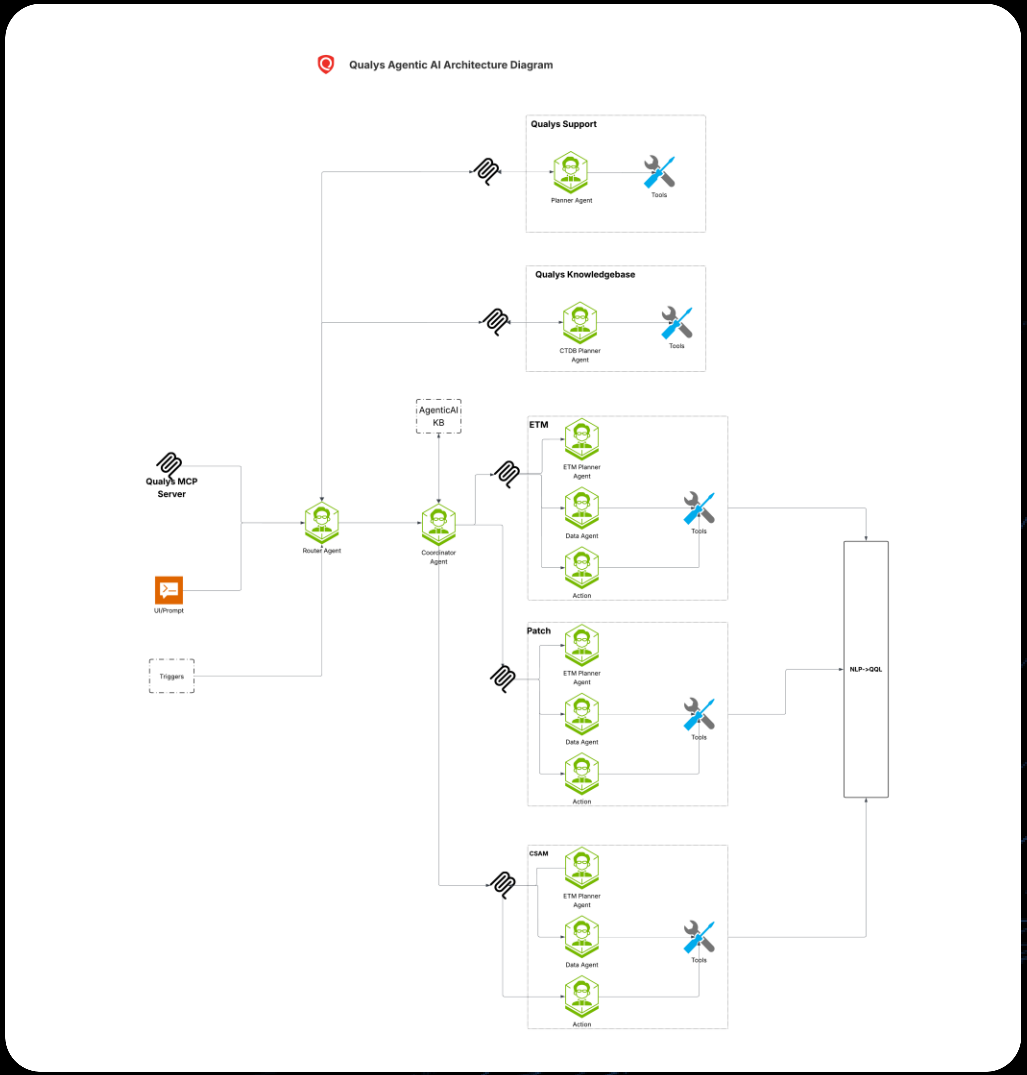
Trigger ▶ Route ▶ Orchestrate ▶ Plan ▶ Execute ▶ Finalize

Architectural Attributes

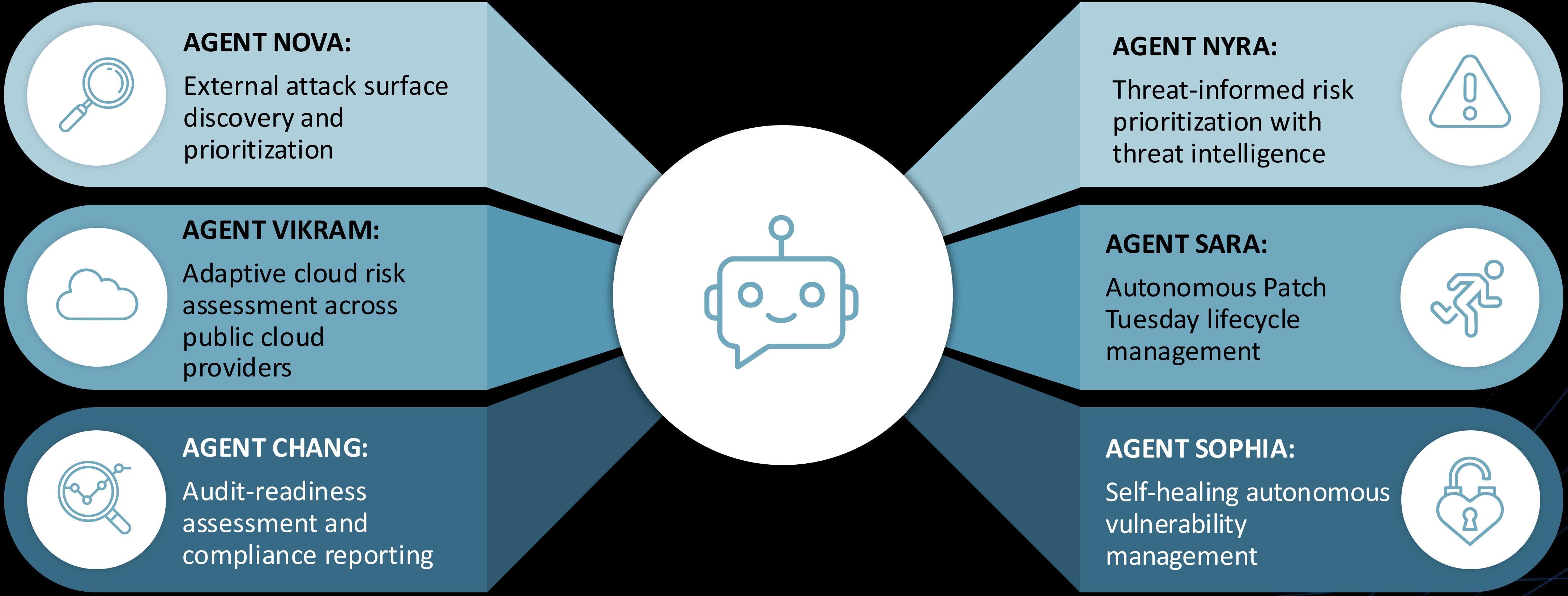
Modularity

Security (JWT)

Extensibility



Specialized Cyber Risk Agents



AGENT NOVA:

External attack surface discovery and prioritization

AGENT VIKRAM:

Adaptive cloud risk assessment across public cloud providers

AGENT CHANG:

Audit-readiness assessment and compliance reporting

AGENT NYRA:

Threat-informed risk prioritization with threat intelligence

AGENT SARA:

Autonomous Patch Tuesday lifecycle management

AGENT SOPHIA:

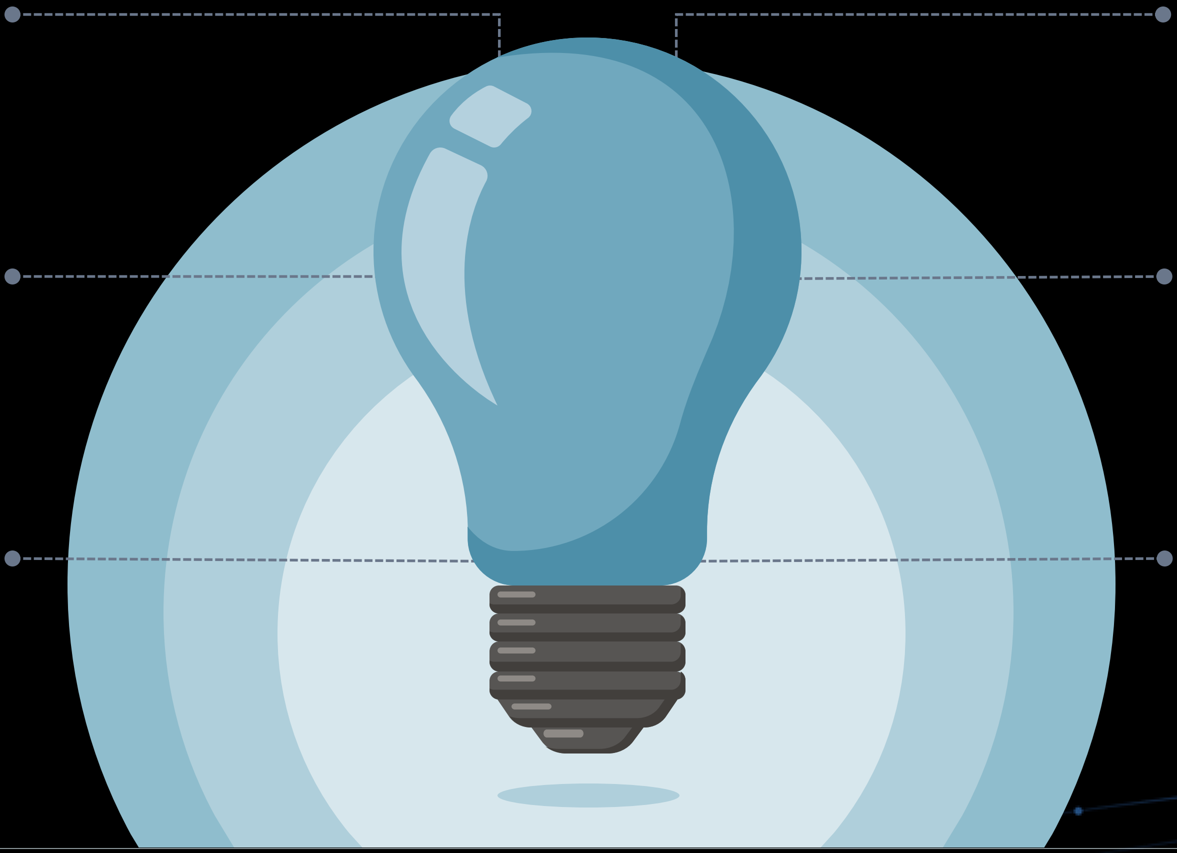
Self-healing autonomous vulnerability management

Key Business Impact & Benefits

Democratized Data Access
Streamline fragmented security data exploration

Enhanced Productivity
Reduce MTTR through autonomous risk reduction

Intelligent Decision Support
Transform data into ranked, actionable insights



Cost Optimization
Focus security teams on strategic initiatives

Proactive Security
Shift from reactive measures to proactive strategies

Measurable ROI
10,000-20,000 hours saved per audit (Agent Chang example)

Getting Started with Agentic AI

ASSESSMENT AND PLANNING

- Evaluate current vulnerability management maturity
- Identify high-impact use cases for agent deployment

AGENT DEPLOYMENT

- Start with pre-built agents from marketplace
- Use no-code builder for custom agents

INTEGRATION & OPTIMIZATION

- Integrate with existing SIEM/SOAR tools
- Continuous learning and adaptation

The Future of Autonomous Cybersecurity

Key Takeaways

- Agentic AI transforms vulnerability management from reactive to autonomous
- Proven architecture with measurable business impact
- Ready-to-deploy agents for immediate value
- Scalable platform for future security challenges

Oracle AI Data Platform

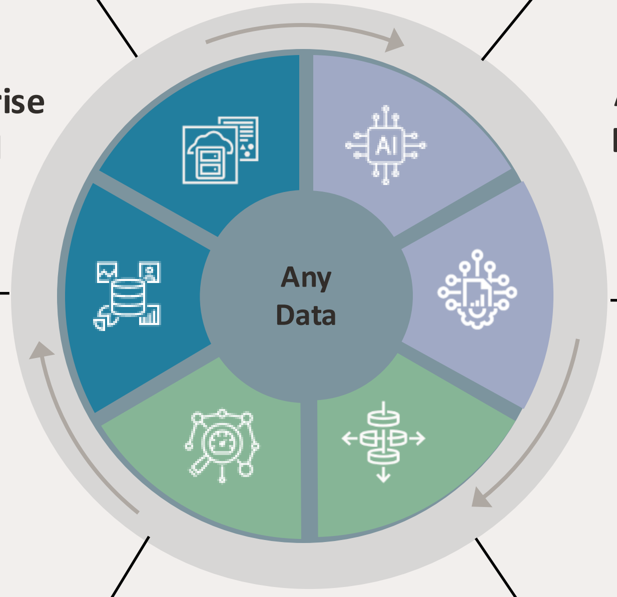
Accelerating AI across the enterprise

Master Catalog: Simplified governance for the entire data estate, including AI and Analytics assets

- Single catalog for data & AI assets
- Role based access control (RBAC)
- Lineage & data quality

Unified Data: A complete connected view of all data from internal apps to external sources like suppliers and partners

- Medallion architecture
- Open data formats
- Pre-built connectors



Unify Enterprise Data for AI

Accelerate AI Development

Innovate with AI at scale

High performance data processing at scale: Open-source flexibility and enterprise-grade proprietary technologies

- Oracle + Open-Source engines
- Multi-development language support

AI powered developer experience: Build data and AI Apps, orchestrate pipelines and accelerate prototypes into production.

- Single pane of glass for all data roles
- AI Code Assist

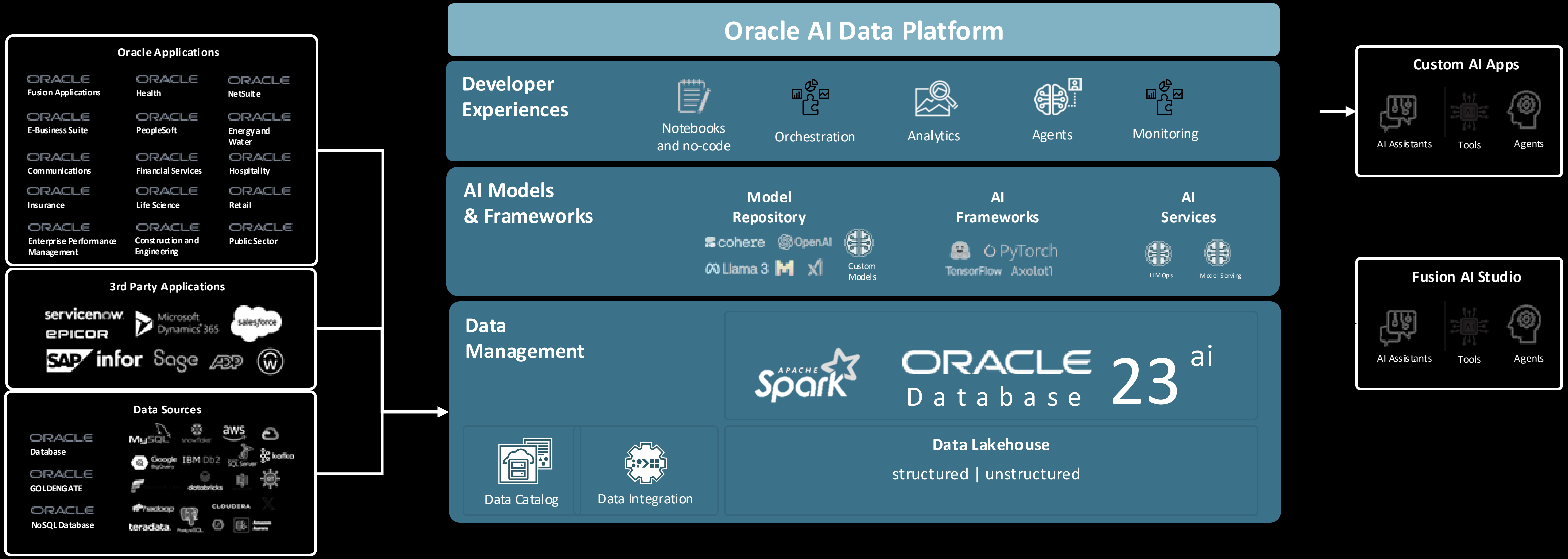
AI Models and Agents: Accelerate the creation of intelligent, enterprise-ready AI Apps.

- Foundational models
- Custom model libraries
- AI Agent flow frameworks

Business Apps and ecosystem Integrated: Native interoperability with Oracle and leading 3rd party services.

- Database and Applications
- Native GoldenGate and FDI integration
- Orchestrate with Fusion AI Studio

Oracle AI Data Platform



Oracle Applications

ORACLE Fusion Applications | ORACLE Health | ORACLE NetSuite

ORACLE E-Business Suite | ORACLE PeopleSoft | ORACLE Energy and Water

ORACLE Communications | ORACLE Financial Services | ORACLE Hospitality

ORACLE Insurance | ORACLE Life Science | ORACLE Retail

ORACLE Enterprise Performance Management | ORACLE Construction and Engineering | ORACLE Public Sector

3rd Party Applications

servicenow, EPICOR, Microsoft Dynamics 365, salesforce, SAP, infor, Sage, ADP, W

Data Sources

ORACLE Database, ORACLE GOLDENGATE, ORACLE NoSQL Database, MySQL, snowflake, aws, Google BigQuery, IBM Db2, SQL Server, kafka, databricks, hadoop, CLOUDERA, teradata, PostgreSQL

Oracle AI Data Platform

Developer Experiences

Notebooks and no-code | Orchestration | Analytics | Agents | Monitoring

AI Models & Frameworks

Model Repository: cohere, OpenAI, Llama 3, M, xAI, Custom Models

AI Frameworks: PyTorch, TensorFlow, Axolotl

AI Services: LLM Ops, Model Serving

Data Management

APACHE Spark | ORACLE Database 23ai

Data Catalog | Data Integration

Data Lakehouse

structured | unstructured

Custom AI Apps

AI Assistants | Tools | Agents

Fusion AI Studio

AI Assistants | Tools | Agents

Unify Enterprise Data for AI

Seamless access to Oracle Application Data, built in governance and lineage, and unified lakehouse architecture for all data types

Accelerate AI App Dev

A single pain of glass and AI tooling for building and deploying custom AI Apps and agents

Innovate with AI at Scale

Leading pricing performance and cross-cloud agent orchestration

Oracle AI for Data is fully Open

We integrate with all the leading LLMs, embedding models, development tool chains, agentic frameworks, etc.

OCI Generative AI	Cohere	OpenAI	Google	Anthropic	Meta	Grok
Hugging Face	Microsoft	Amazon Bedrock	Mistral AI	Jina AI	Qwen	LAION
LangChain	ONNX	LangGraph	Pytorch	Ollama	Haystack	TensorFlow

You can use your preferred models and tools

Executive Summary

Oracle AI Data Platform provides Apache Spark and Oracle 23ai as an Engineered Data Platform

Oracle 23ai Multi-Cloud Database delivers key features required to design your AI Strategy

- Knowledge Graph
- Vector Search
- Support for Multi Datatypes (Json, Spatial and Structured)
- In Database Machine learning and AI
- Multicloud options(OCI, AWS, GCP and Azure)
- Applied AI Studio

Oracle Integration Solutions

- Oracle Integration Cloud (Zero-ETL and OOB connectors to 450 data sources)
- Golden Gate (1000+ OOB connectors for Data Replication)

Oracle GenAI, Agent and Data Science service provides

- LLM Models
- Out of box tools(RAG and Nl2SQL)
- Agent development Kit
- BYOM models from Hugging Face