Research Note
BY RICHARD WINTER

Oracle AI Database and Agentic AI

Secure, Practical Agentic AI for the Enterprise

AT ITS AI WORLD TOUR IN LONDON, on March 24, Oracle announced a major set of new capabilities for Agentic AI. Unlike much of what we have seen from other vendors over the past year, Oracle's capabilities are genuinely enterprise-class with a focus on ease-of-use, security, efficiency, scalability, mission-critical requirements and trustable results. For example, Oracle's *AI Database Private Agent Factory* is a GUI-based, no code platform for business users to create, test and deploy intelligent data-centric agents and workflows safely and securely in the cloud or on prem. The announcement also included a commitment from Oracle to open data: Oracle will now support data in *Apache Iceberg* formats with both vector search and vector indexes, as well as SQL.

Much has been written lately about customers struggling to move AI projects to production and realize business value. These Oracle capabilities remove the obstacles that have been holding many of those projects back and open the door to mission-critical, enterprise-scale use cases for Agentic AI. The result is a remarkably potent new business opportunity for Oracle customers.

Agentic AI

With the new capabilities announced by Oracle, customers can create, deploy and manage intelligent agents that operate with considerable autonomy to accomplish business and/or technical tasks.

At the briefing I attended, Oracle offered the example of a multi-agent application using a workflow to handle customer service for a meal delivery service.

> Suppose you ordered a restaurant meal for delivery at 6:30pm; it has not arrived; and now it is 7:10pm. You contact the meal delivery service and are connected to an ***AI agent***. You can speak to it in English (or whatever language you prefer to speak) and it can understand you and reply. But, unlike general purpose chatbots, it can carry out and coordinate actions among agents and follow appropriate business procedures: check on the status of your order and update you; handle a cancellation if you want to cancel; process a refund if your order arrives late; handle a complaint and arrange appropriate follow up; and, apply the company's policies to each of the processes (so, for example, if the delivery person arrived at 6:30pm and no one was home to accept delivery, you may not be entitled to a refund).

In a traditionally programmed business application, the system can handle only the specific inputs, conditions and exceptions that the programmer has explicitly anticipated.

WinterCorp
www.wintercorp.com

WINTERCORP RESEARCH PROGRAM

Methodology

PURPOSE AND METHODOLOGY FOR THIS REPORT

This *WinterCorp Research Note* covers Oracle's recent announcement of *Oracle AI Database Agrntic AI,* related developments and their implications for customers. In creating this report, WinterCorp drew on its own independent research and experience, interviewed employees, attended Oracle events and analyzed Oracle documentation and literature. Oracle, in its capacity as the sponsor of this report, was provided an opportunity to comment on the paper with respect to facts. WinterCorp has final editorial control over the content of this publication and is solely responsible for any opinions expressed.

Intelligent agents are more like self-driving cars: they are given goals and guidelines and plot their own path to the destination or coordinate with other agents… and they learn, evolve and improve over time. They can typically handle exceptions that were not specifically planned for. As a result, it takes less time and effort to create the typical business solution. Better yet, the resulting process will often be more robust and require less maintenance effort than with previous technologies.

Pre-Built Agents

To help customers become familiar with what Agents can do and how they work, Oracle is providing some pre-built Agents with its *AI Database Private Agent Factory*. Three examples are:

- **Knowledge Agent** – applies vector search to enterprise data to search on concepts and similarity;
- **Data Analysis Agent** – understands the database schema and extracts semantic insights from structured data, taking business context into account; and,
- **Deep Research Agent** – goes deeply into a subject to analyze more complex issues.

These are agents that can search and analyze a wide variety of enterprise data and information resources (documents, images, graphs, etc.), answer questions, analyze data and decompose questions into sub-questions.

AI Database Private Agent Factory

Customers, including business users, can build their own agents with Oracle's new *Private Agent Factory*. This is a no code platform in which the agent and its workflow are composed on a canvas with a drag and drop interface. The resulting agent has full access to the *Oracle AI Database*, subject to security and governance constraints, and can be deployed anywhere that *Oracle AI Database* runs: on prem, in private cloud, in *Oracle Cloud Infrastructure (OCI)* or in major hyperscaler clouds such as *AWS*, *Azure* or *Google Cloud*. Because the agent is created — and operates — in a private container, it is secure in all of these environments.

Unified Agent Memory Core

To function effectively, agents need both short-term and long-term memory of context and sessions. This memory is crucial to their ability to learn and improve, which is central to their business value. And agents need to remember all types of information: text, images, audio, structured data and so on. Most of the popular data platforms on the market today were designed for query and analytics on structured data, not for the broad requirements of agentic memory. Oracle stands alone in that it has been developing and architecting a converged database for decades. As a converged database, it is explicitly designed to manage virtually all types of data, all types of operations on data and all types of development styles. So, while most vendors are adopting additional engines or connecting to external ones to act as the agentic memory, Oracle is able to meet this requirement with its existing database, streamlining and simplifying agentic architecture and application deployment.

Autonomous AI Vector Database

While Oracle delivered vector support some time ago, its full range of vector-related capabilities are now available as ***Autonomous AI Vector Database***. This includes a vector data type; vector embedding; vector indexing; and vector search by means of extensions to SQL. Because the vector capabilities are fully integrated with SQL and with the database, semantic search can be combined in a single SQL statement with structured database search terms; JSON-search; and all the other capabilities of Autonomous AI Database. What's more, these are implemented to work well at large-scale, while the standard techniques used elsewhere often do not.

Autonomous AI Vector Database provides a lower cost entry point for developers and data scientists to quickly and easily build vector-powered applications using intuitive APIs and an easy-to-use web interface. In contrast to other specialized vector database offerings which only know vectors, customers can upgrade to *Autonomous AI Database* with one-click when their requirements grow. A further advantage is that the vector capabilities are delivered on a foundation that is mature and has benefitted from decades of use by customers in a wide range of applications.

This brings a critical advantage to Oracle customers, who already have their business data in Oracle databases. They are thus able to bring AI capabilities — including vector-based semantic search — to their data, rather than having to move their data to another database.

Deep Data Security

AI greatly increases the risk of exposing sensitive data. This is because many customers depend on application-level controls to limit access to sensitive data, while many new AI-based solutions bypass the applications and go directly to the database. An agent can often generate any SQL query; if it does not have the same built-in controls as the applications it is bypassing, the sensitive data can and will be exposed.

Oracle Deep Data Security avoids this by offering granular control of data privacy policies at the database-level. Oracle supports role-based security at the table, column, row and cell level. It also provides complete capabilities for data encryption and masking. Think of it as guard rails for agents — they can only access the data that you actually want them to, versus whatever they try to access on their own accord — or what some malicious actor activated them to do. Deep Data Security will become increasingly critical as the AI era enters into full-scale AI production workloads.

Trusted Answer Search

Generative AI provides the remarkable capability to answer virtually any question by searching your enterprise data and documents. Unfortunately, at present, these answers are not always correct. Even questions answered correctly today can be answered incorrectly at some point in the future as the LLMs, the data and the context information evolve.

Though the percentage of correct answers is quite high — often well over 95% — "quite high" is not good enough for many enterprise uses.

In response, Oracle has introduced ***Trusted Answer Search***. This is a facility built directly into *Oracle AI Database* whereby end-user natural language questions are matched to previously created reports. By instituting a process whereby production reports are certified as correct by their stakeholders before approval for production use, customers can create a class of Trusted Answers. This approach uses *Oracle AI Vector Search* rather than an LLM to find the answer to the question. The entire Trusted Answer process is overseen by a Search Admin which manages access, learns from user feedback, tests queries, does regression analysis on the questions and test answers and reviews query history.

Open Table Formats: No Vendor Lock In

Oracle AI Database supports Open Table Formats, including *Apache Iceberg*, *Delta Lake* and *Parquet*. Data in these formats can thus be accessed directly both by *Oracle AI Database* and by other query engines and analytical tools. Now organizations can run *Oracle* apps, AI, tools and analytics on *Iceberg* data and run *Iceberg* apps, AI, tools and analytics on *Oracle* data. They can also run real-time OLTP and mixed workloads on *Iceberg* data and choose the best query engine on a query-by-query basis, as well as select data storage on a case-by-case basis and easily shift back and forth.

Vectors on Ice

With this latest announcement, Oracle has extended its Open Table support to include vector embedding and vector search for data in *Iceberg Table Formats*. The vectors can be stored either in the *Oracle AI Database* or in *Iceberg Tables* in object storage. Either way, *Oracle AI Database* will support semantic search on the vectorized Iceberg Table data, bringing a level of performance to open data that would otherwise not be available. Clearly, Oracle's focus on collaboration, openness and flexibility continues with this latest announcement.

About WinterCorp

WinterCorp is an independent consulting firm expert in the strategy, architecture and scalability of the modern analytic data ecosystem, focusing on enterprise AI at scale.

Since our founding in 1992, we have architected and engineered solutions to some of the toughest and most demanding analytic data challenges, worldwide.

We help customers define their AI and data-related business interests and vision; quantify their AI-related workloads and data platform requirements; develop their data strategies and architectures; select their data platforms; and engineer their solutions to optimize business value and obtain otherwise infeasible business outcomes.

Our customers get business results with analytics and AI in which their return is often ten or more times their investment.

When needed, we create and conduct simulations, benchmarks, proofs-of-concept, pilot programs and system engineering studies that help our clients manage profound technical risks, control costs and reach business goals.

With our in-depth knowledge and experience, we deliver unmatched insight into the issues that impede scalability, and into the technologies and practices that enable business success.

WinterCorp
www.wintercorp.com
TYNGSBORO, MA
617-695-1800

Open Agent Spec

Intelligent agents are emerging as the new interface to enterprise data. It is clear that most customers will soon be running agents that come from multiple sources, if they are not doing so already. Yet, there is no generally accepted way to create agents in one vendor environment that can definitely be expected to work with the products of another vendor.

The industry needs a standard, so Oracle has proposed one named the *Open Agent Specification*. This is a language that defines the internal structure of an agent and its work-flow, enabling agents to be portable across platforms. It supports standards such as MCP and A2A. You can think of it as SQL for agents.

Recommendation

WINTERCORP RECOMMENDS customers take a close look at the *Oracle AI Database Agentic AI* announcement that took place in London. This is an exciting set of new capabilities, engineered for the enterprise, with attention to security, scalability, trusted answers and manageability.

It features Oracle's long proven, converged database architecture as the agentic memory, probably the best in the industry for that critically important piece of the puzzle. It introduces a no code end user capability for the creation and deployment of agents to handle business processes. And it supports data in open table formats, eliminating vendor lock-in of data.

Intelligent agents are like self-driving cars for business processes — you set the objective and they navigate to it, operating with some autonomy. With *Oracle Unified Agent Memory Core*, they remember what happened and they learn, improving over time. The resulting business systems have the potential to be much more productive, more flexible and produce better outcomes than those that have been developed in the past. So, these new capabilities open the door to great opportunities for Oracle customers. As with any major technical capability, WinterCorp recommends that customers do a thorough evaluation and test any capabilities on which they expect to rely for critical business outcomes.

We are entering an age of AI which promises to enable extraordinary new solutions to business problems. WinterCorp believes that Oracle's newly-announced capabilities for Agentic AI are going to empower many enterprises to realize that promise.