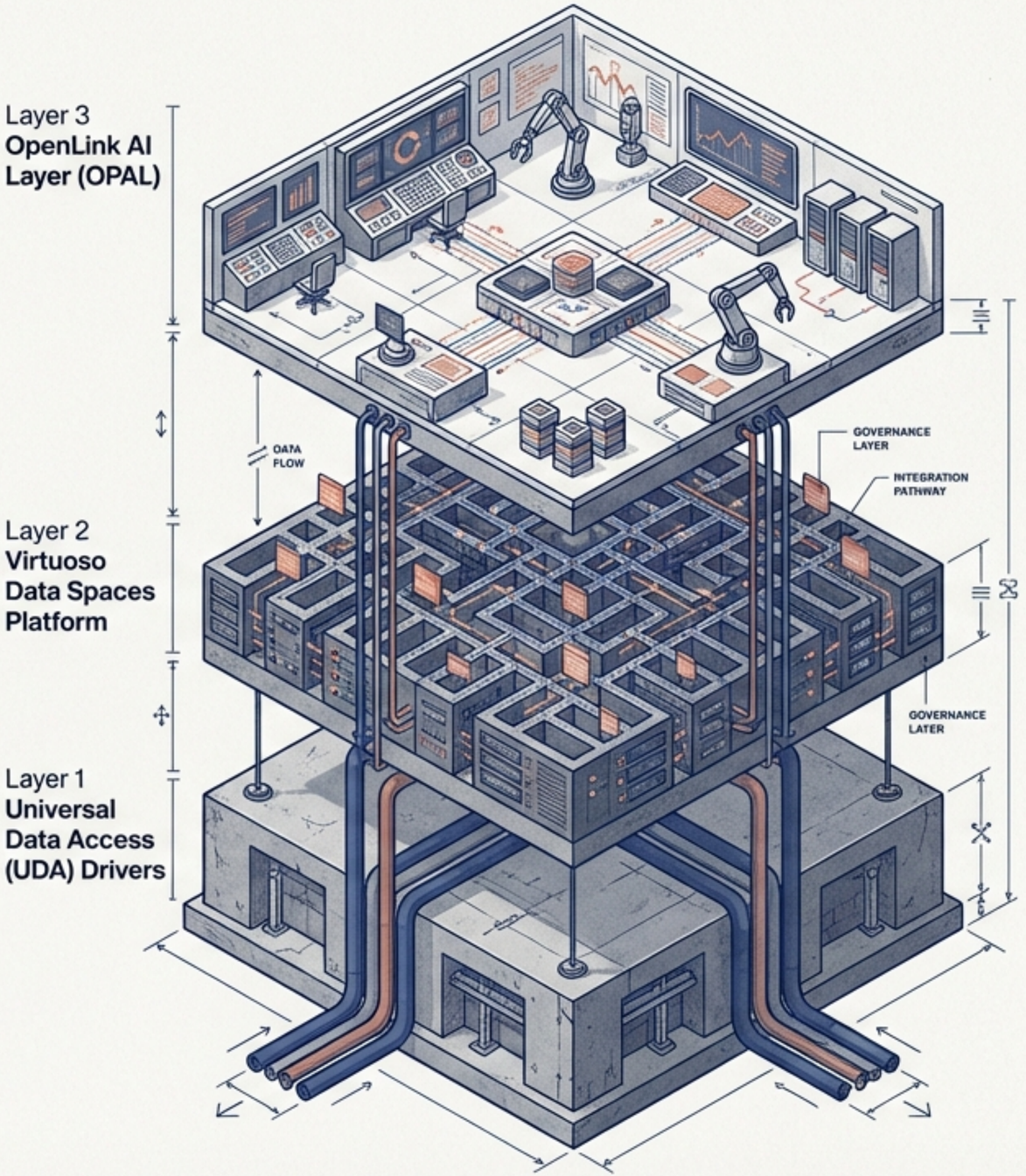
The OpenLink Architecture for Autonomous Enterprise Agents

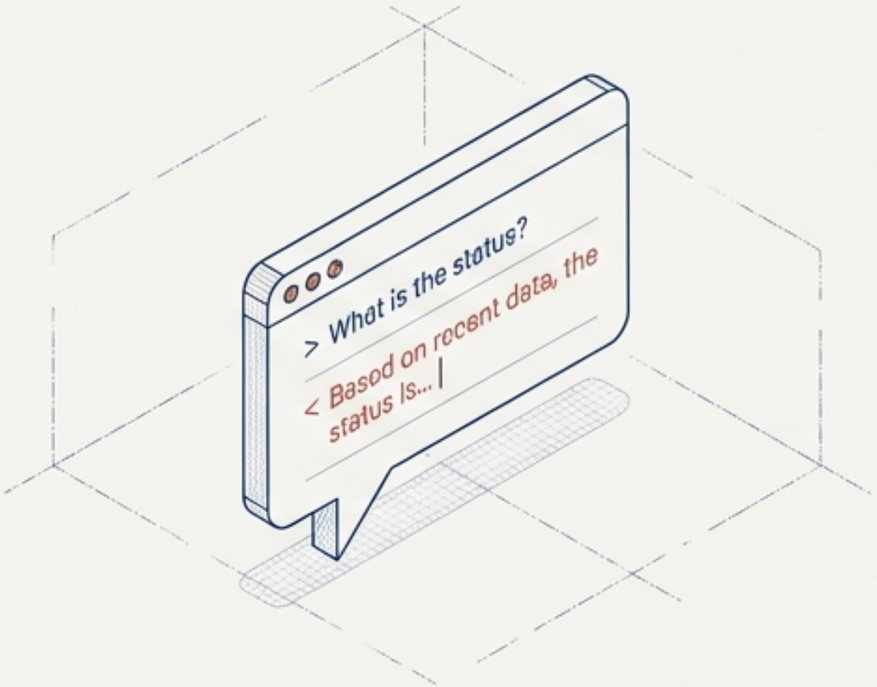
From governed data access to continuously operating, data-aware AI.

AI agents are moving from chat interfaces to operational layers. This requires a vertical infrastructure that ensures agents operate safely, continuously, and functionally within existing enterprise environments.



The shift from conversational models to operational agency

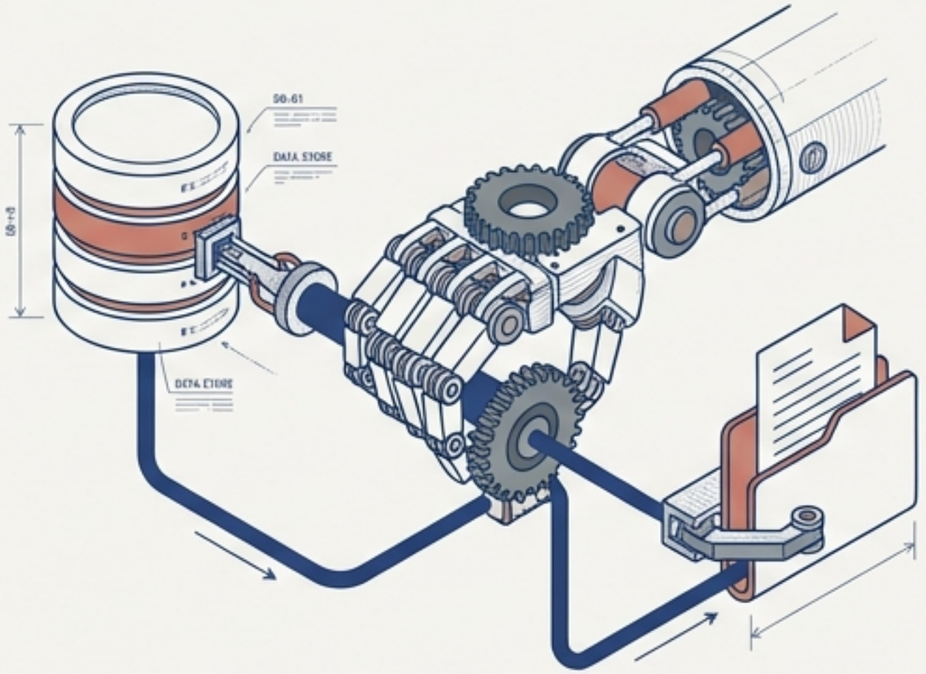
The LLM Era



Conversational Context Only

Chatbots operate in isolation. They lack deep connection to enterprise reality and rely on transient context windows.

The Agentic Era



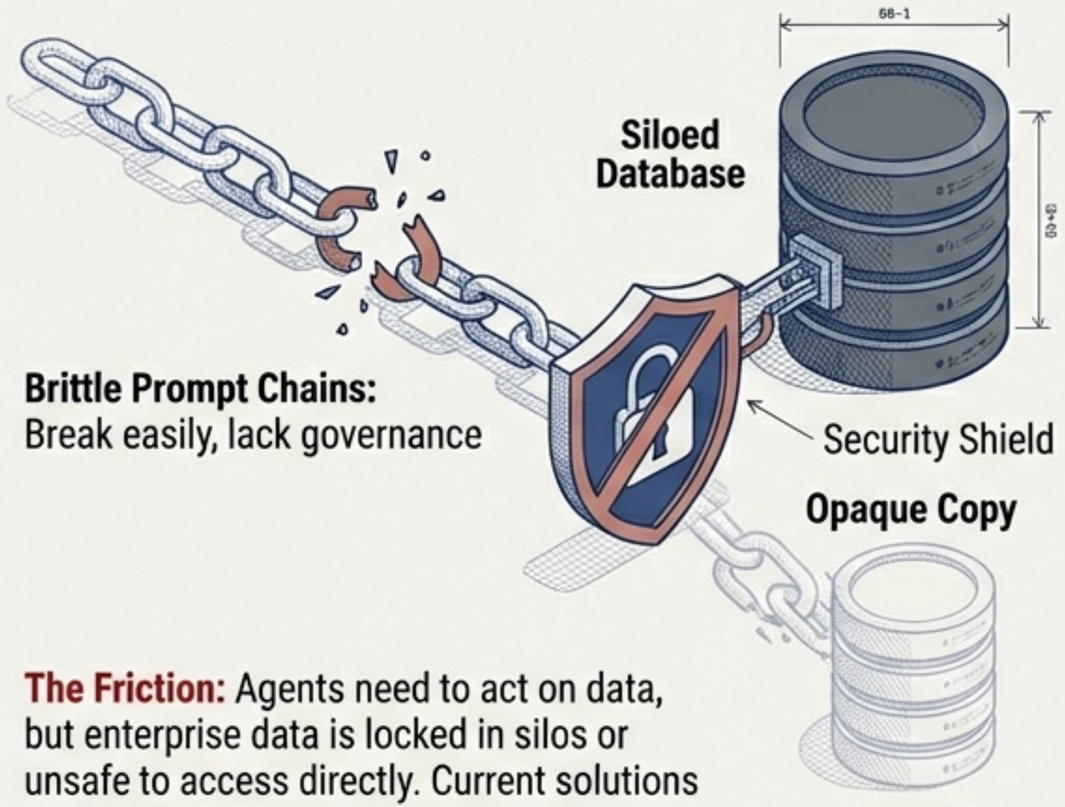
Operational Context & Action

Agents act as an operational layer. They must reason across disparate systems and execute actions directly against data.

The Requirement: To function in production, agents must operate continuously without breaking security protocols or losing context.

True autonomy requires a vertical stack, not brittle chains or opaque copies.

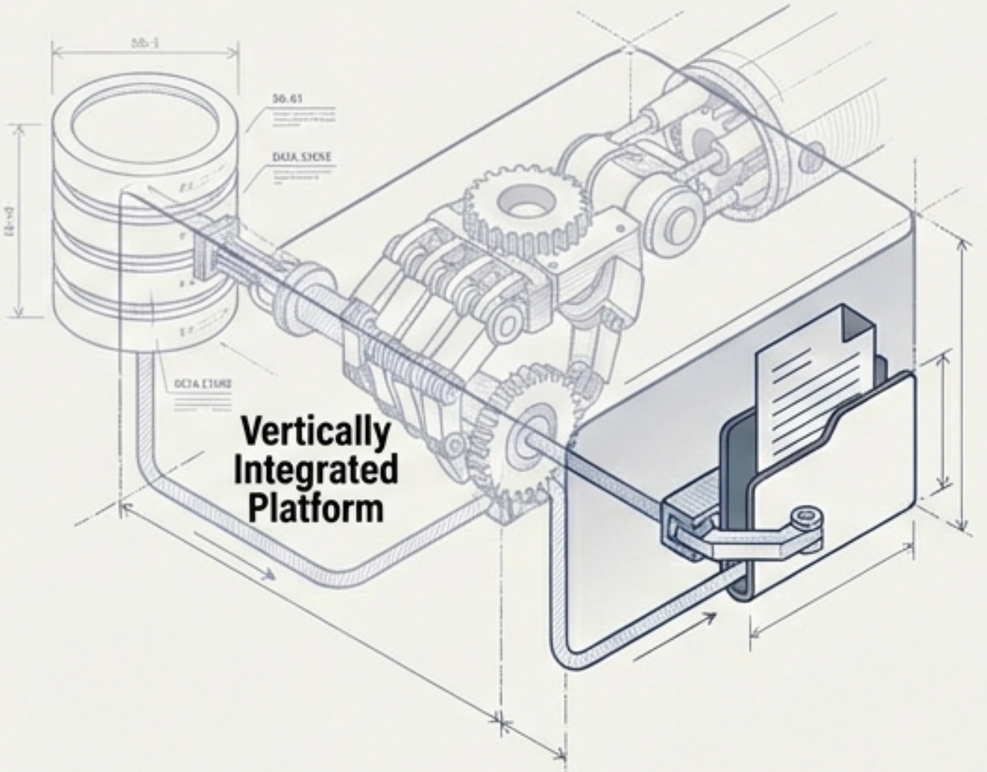
Pathway A (The Status Quo)



Brittle Prompt Chains:
Break easily, lack governance

The Friction: Agents need to act on data, but enterprise data is locked in silos or unsafe to access directly. Current solutions rely on brittle chains or opaque copies.

Pathway B (The Missing Piece)



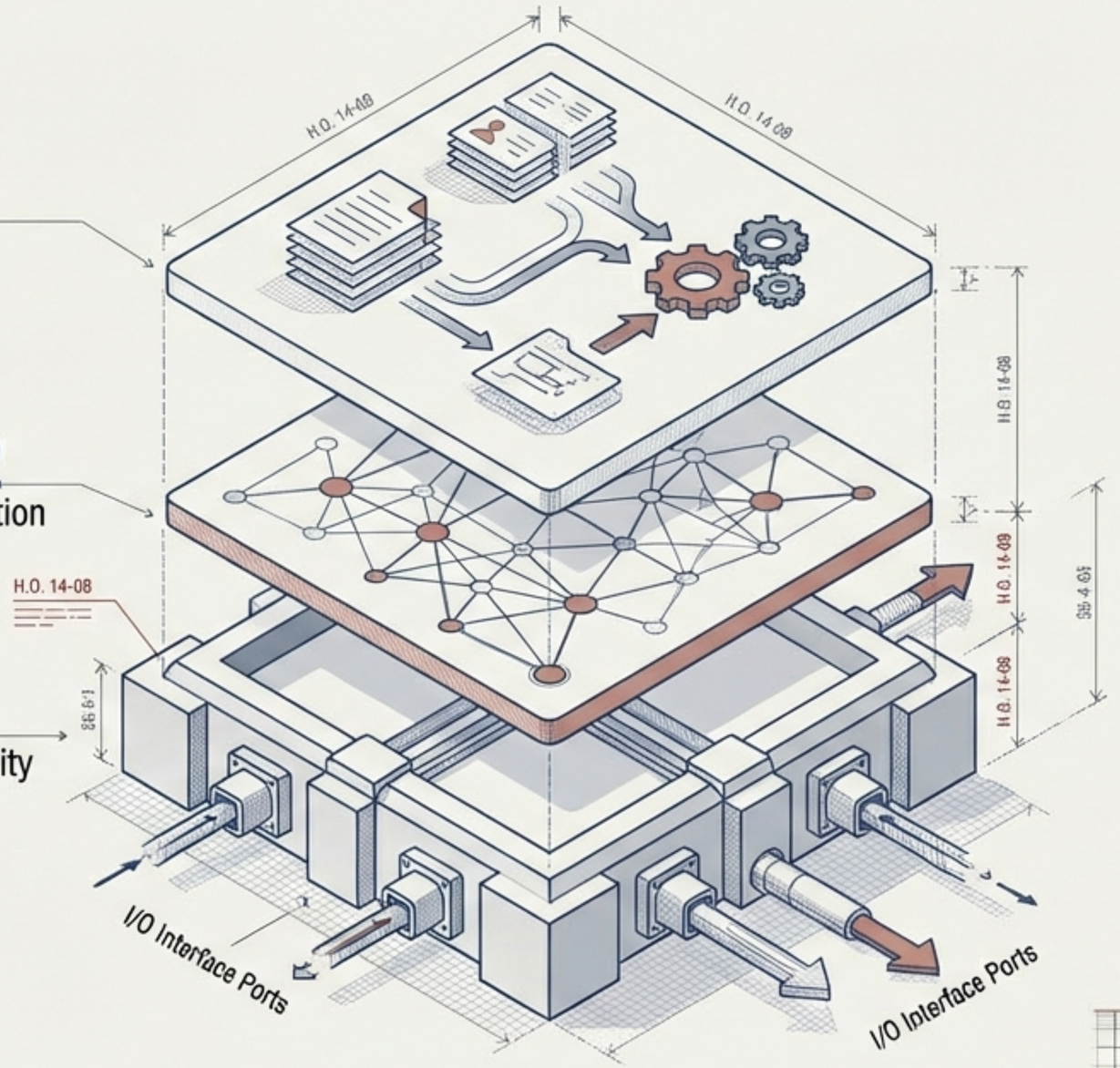
Starts where enterprise reality begins: at the data access layer.

A production-grade stack built on three distinct layers.

Foundation: DBMS-agnostic connectivity with embedded governance.

Middle Tier: Semantic harmonisation that keeps data in place.

Apex: Natural language agents loosely coupled to open standards.

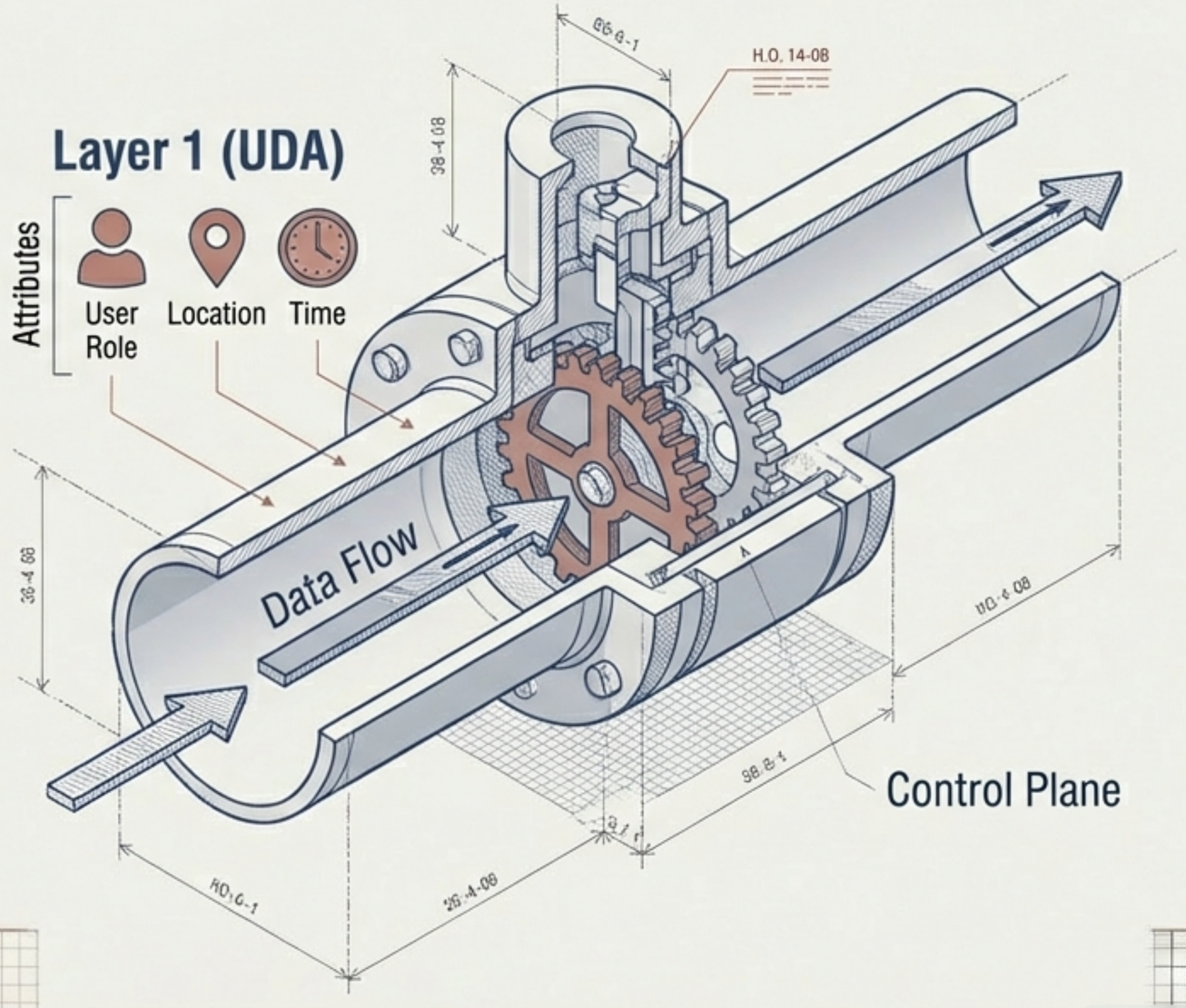


Governance must begin at the point of connection, not be retrofitted downstream.

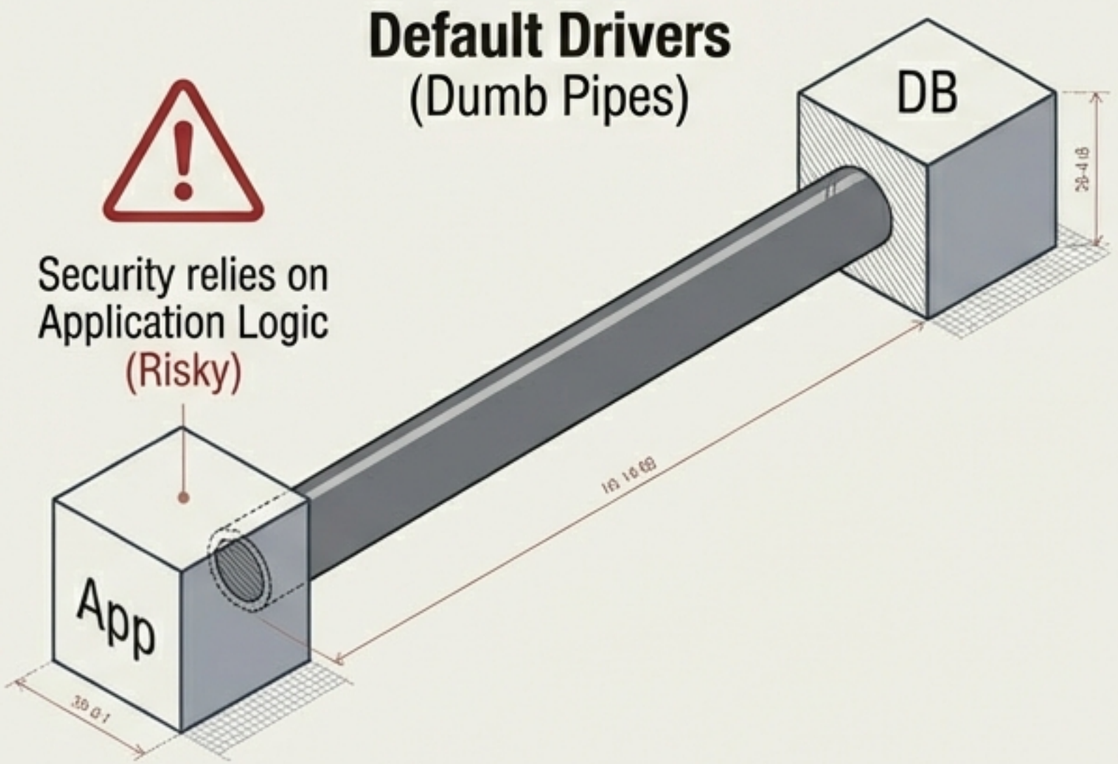
The Technology: OpenLink Universal Data Access (UDA) drivers (ODBC/JDBC).

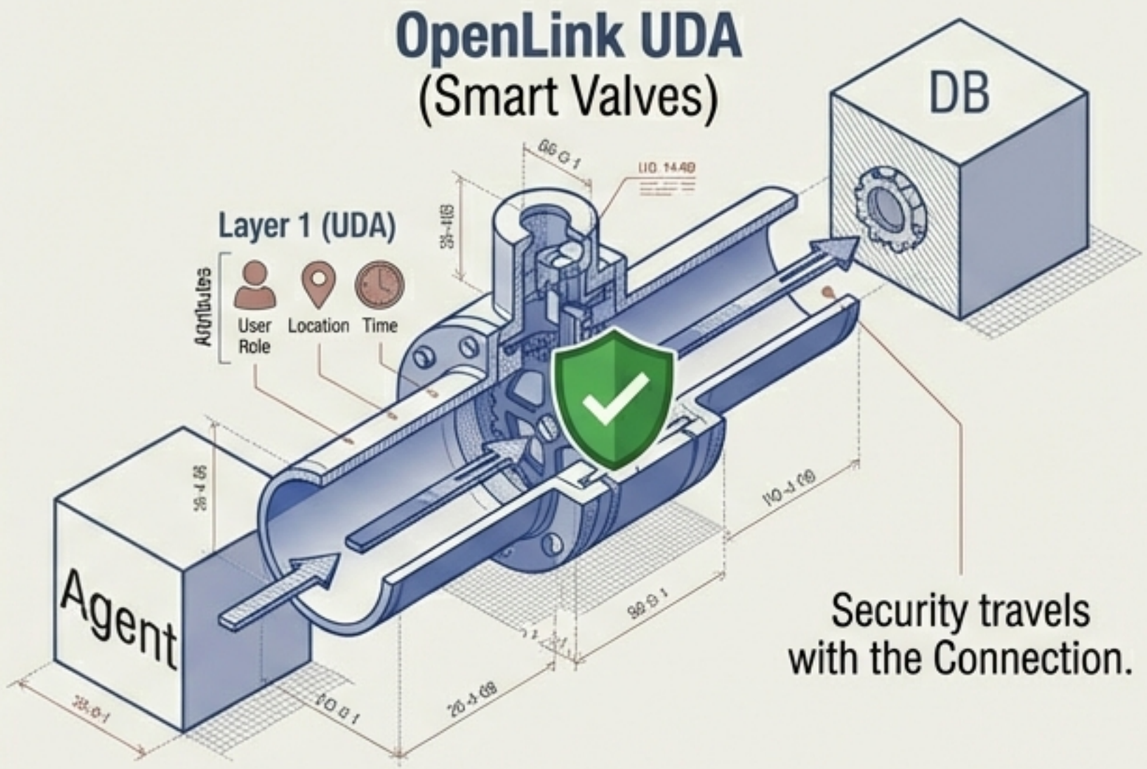
The Insight: Crucially, they introduce a missing control plane. Unlike default drivers, governance is not deferred to the application.

The Mechanism: Fine-grained, attribute-based access control is enforced directly at the data access layer.



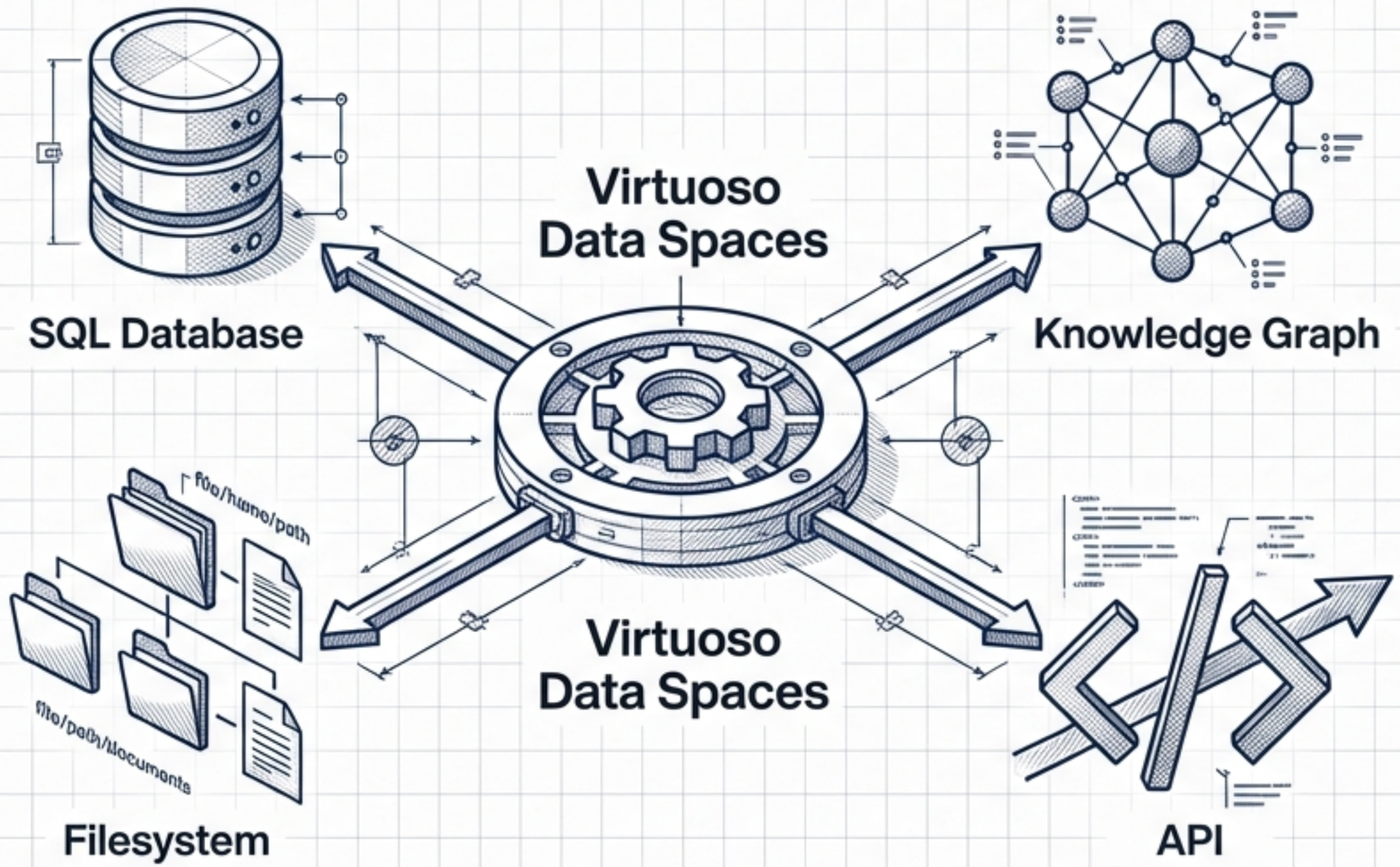
Transforming drivers from passive pipes into active active security enforcement.





Bundled drivers lack governance, leaving security to the app. OpenLink UDA enforces policies at the point of access, ensuring legacy apps and AI agents are subject to the same rigorous auditability.

Turning fragmented systems into a coherent data substrate without rewriting infrastructure



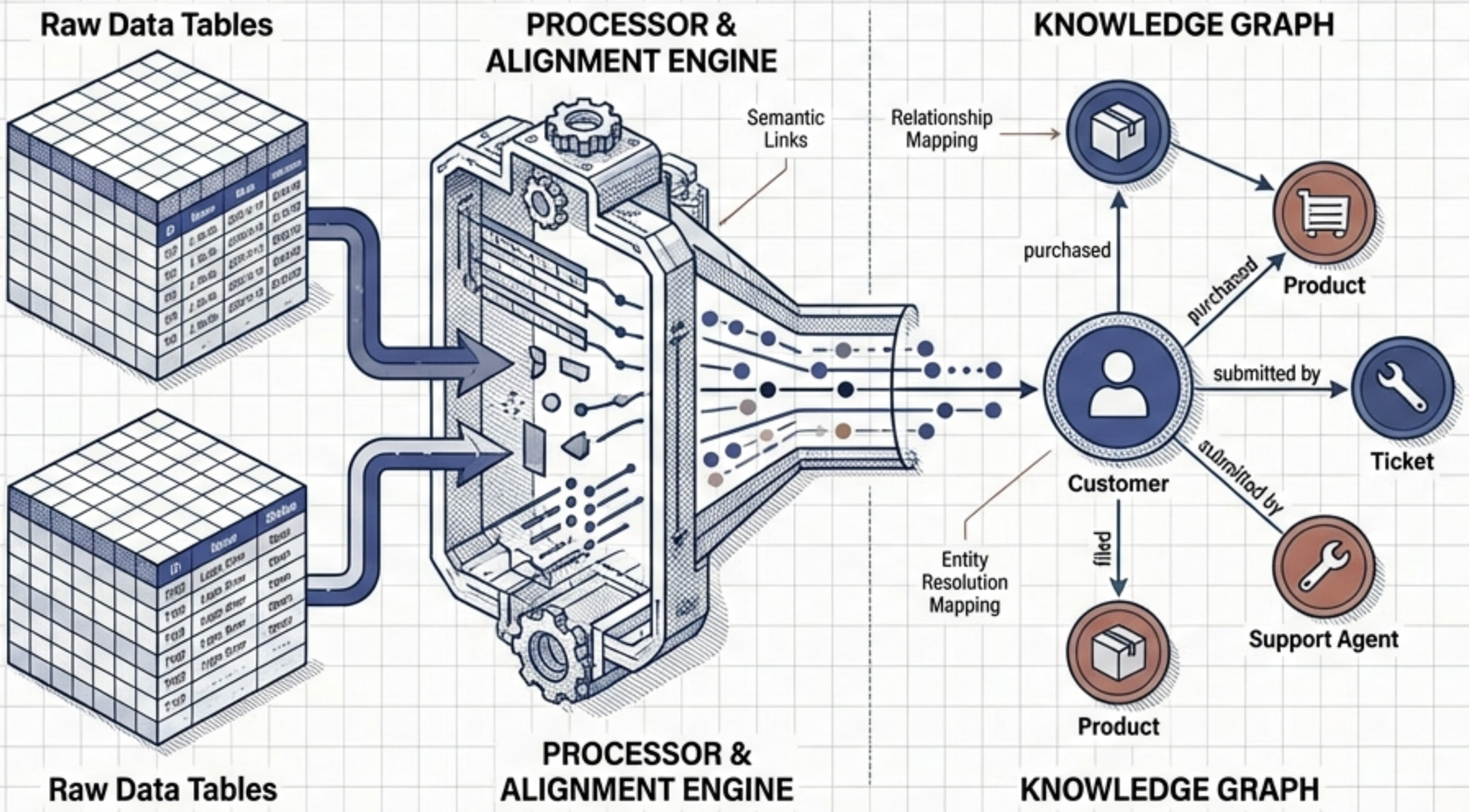
The Strategy

Moves beyond connectivity to provide loose coupling and semantic harmonisation.

The Outcome

Data remains in place. Virtuoso exposes these assets through a unified, standards-based interface, making them interoperable and queryable.

Contextually aligned data enables agents to reason rather than just query.



Contextual Alignment

By harmonising semantics, Virtuoso ensures that when an agent queries "customer", it understands the relationship between the billing record (SQL) and the support ticket (API).

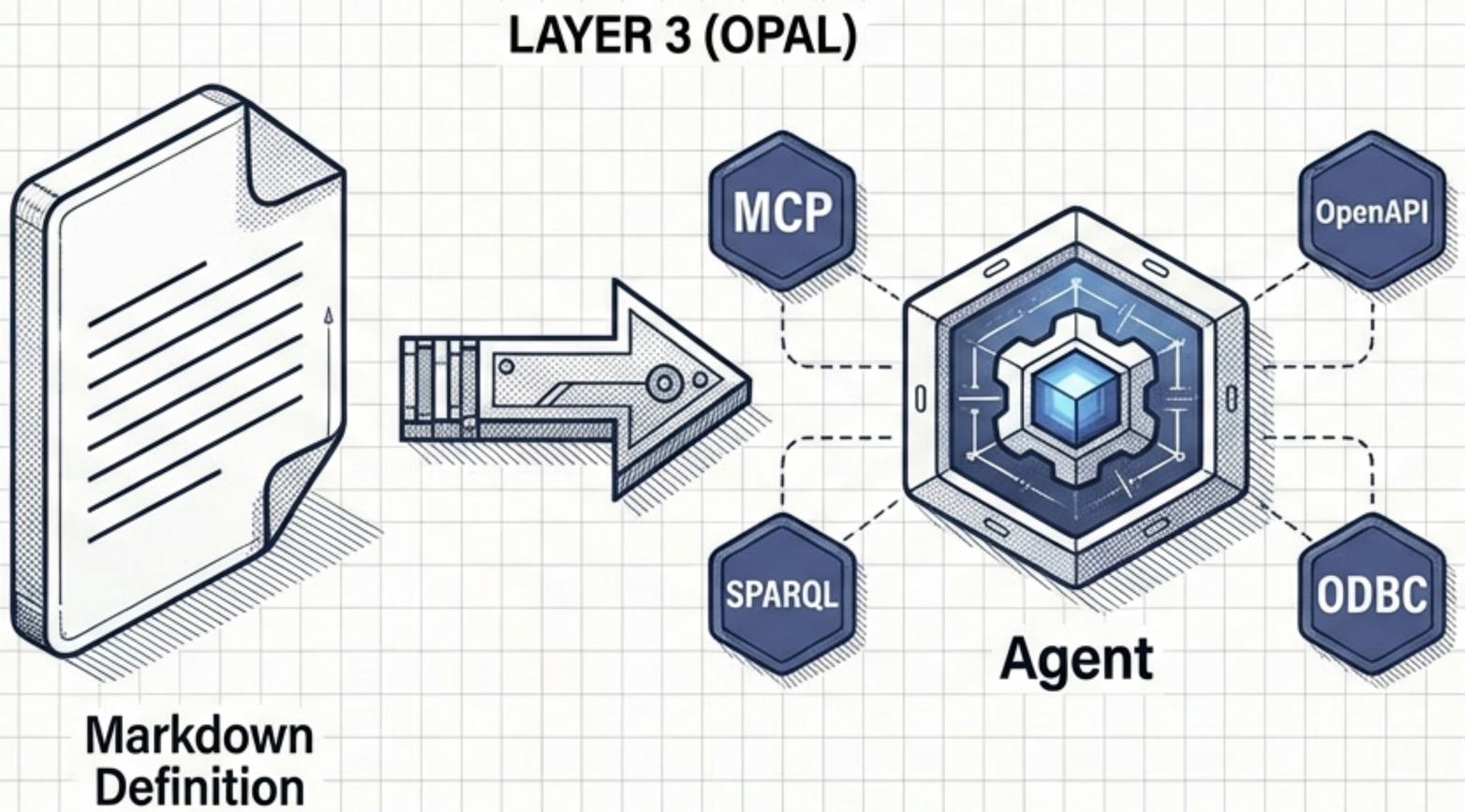
No Consolidation

Transforms fragmented systems without forcing consolidation or expensive rewrites.

Standardisation

Agents interact with the enterprise landscape using standard protocols.

Decoupling agents from proprietary runtimes using open standards.

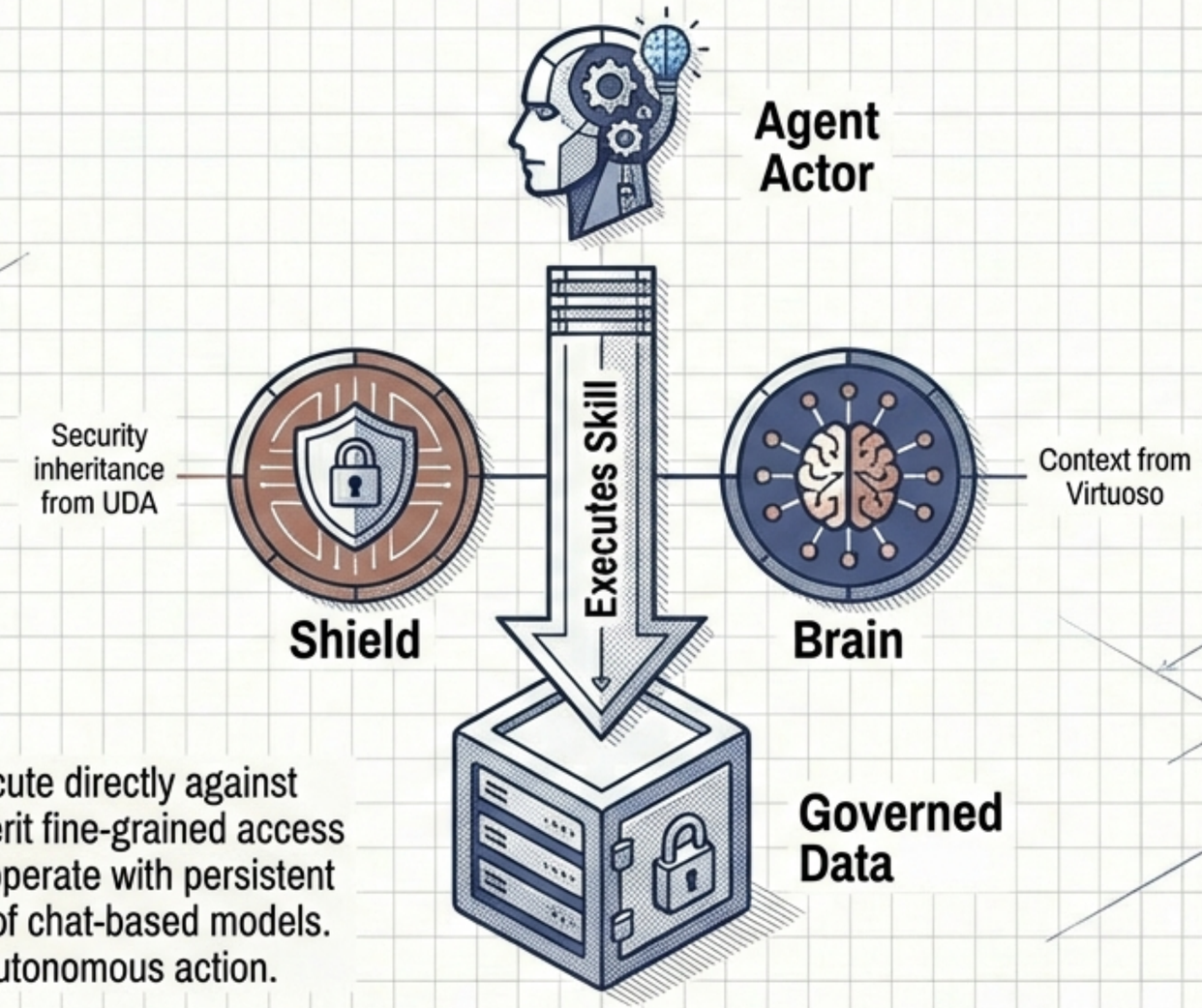


The Technology: OpenLink AI Layer (OPAL).

The Definition: Enables the development of AI agents using natural language expressed in Markdown.

Freedom from Lock-in: OPAL agents are not tightly bound to proprietary runtimes. They are loosely coupled to data spaces through open standards.

Executing skills with persistent, auditabe context.



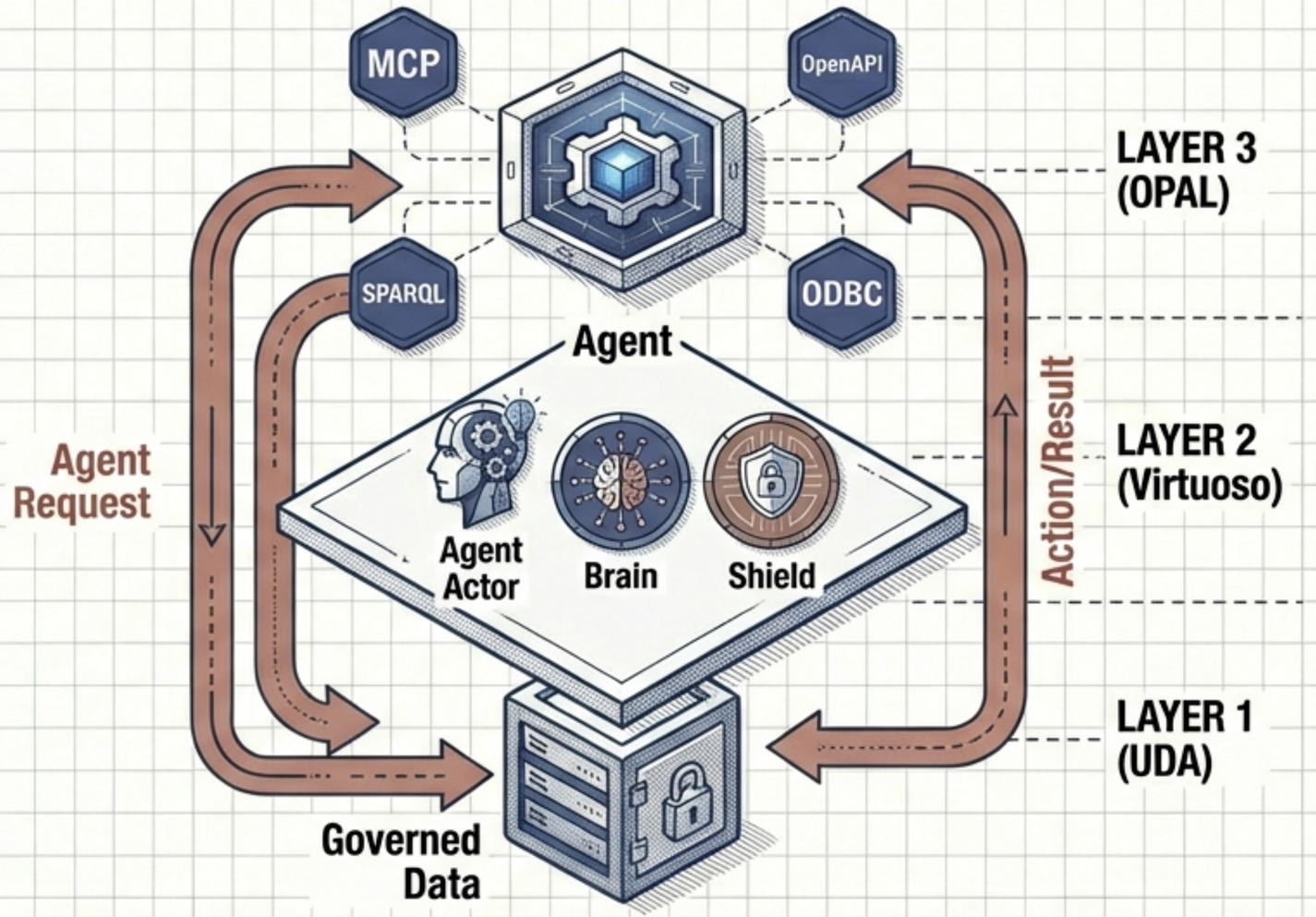
Skill Execution: Agent skills execute directly against governed data in place. They inherit fine-grained access controls from the UDA layer and operate with persistent context, eliminating the amnesia of chat-based models. The result is auditable and safe autonomous action.

A complete vertical stack for production-grade agentic systems.

Integrated Workflow: The three layers work in unison to allow reasoning over live enterprise data.

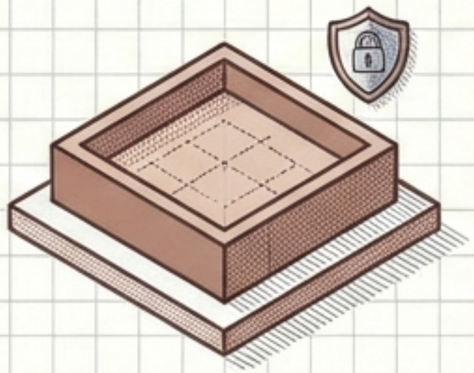
Coordination: Agents can coordinate actions across systems naturally.

First-Class Actors: Existing applications remain intact, while agents become first-class actors within the enterprise architecture.



An architecture that scales naturally with organisational maturity.

This approach aligns AI adoption with the way enterprises already manage data, security, and operations.



Experimentation

Safe sandboxing via UDA control plane.

Production

Semantic coupling resists breaking changes.

Evolution

Open standards ensure long-term adaptability.

Delivering AI systems that enterprises can trust to reason, decide, and act.

The End-to-End Narrative

From governed data access...

To semantically harmonised data spaces...

To continuously operating, data-aware AI agents.