Vendor Coverage Diagnostic

Assessed against the Agentic AI Capability Stack™

Frédéric Verhelst · Version 1.1 · Q2 2026

In brief. What each solution category can enforce, and on whose standards. Page 1 sets out why ownership matters; page 2 maps current vendor coverage; page 3 gives the operating pattern and the six contract tests for your next platform decision.

Purpose

Assessed against the *Agentic AI Capability Stack™*, Version 3.1. The matrix scores the seven capabilities where vendor coverage diverges, Capabilities 3 to 9. Vendors named are established examples, not a comprehensive market survey; inclusion does not constitute endorsement. Reviewed quarterly.

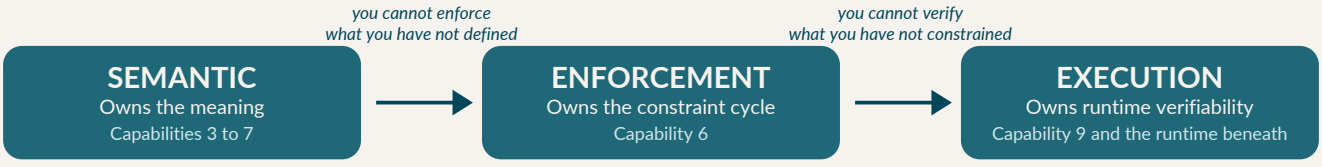
The eleven capabilities

Cap.	Name	What it does
11	Strategy	The board mandate and the investment case for AI
10	Operating Model	Who decides what: human and agent roles, decision rights, escalation
9	Agent Capability	The agents themselves: how they run, coordinate, and act
8	Agent Connectivity	One common way for agents to reach tools and governance
7	Provenance	An auditable record of which data, rules, and authority produced each action
6	Guardrails	Rules checked before an agent acts, not after the fact
5	Agent Contracts	What each agent is permitted to do, stated so machines can enforce it
4	Knowledge Graph	The connected, queryable record of the organisation's knowledge
3	Ontology	The agreed meaning of the organisation's terms, so every agent reads them the same way
2	Data Connectivity	The pipelines and event streams that move data into the stack
1	Data	The organisation's data and authored knowledge, structured and unstructured

Capabilities 1–2 and 10–11 are not vendor-differentiated: data foundation is commodity infrastructure; strategy and operating model are board mandate. Capabilities 3 through 9, marked at left, are the governance and capability core scored on page 2, where coverage diverges and ownership determines sovereignty.

Why ownership matters

Three links, one chain. Each link is the precondition for the next.



Lose any link and it collapses to whoever owns the missing one, almost always the vendor.

The chain is a procurement test, not an architecture diagram. **Semantic sovereignty** asks whether the organisation, not the vendor, owns the meaning its agents reason over. **Enforcement sovereignty** asks whether a change in regulation can be applied on the organisation's own schedule or only when the vendor ships a release. **Execution sovereignty** asks whether the organisation can verify, independently of the provider, that an agent did what it was told. Each is a question about who holds the capability when the vendor relationship changes, and each points to a different requirement when technology is chosen.

These three coverage links rest on a fourth the matrix does not score, because it is a question of where a platform runs, not what it covers. **Jurisdictional sovereignty** asks whether a third party can compel your provider to cut access. In June 2026 a US export-control directive forced Anthropic to disable Fable 5 and Mythos 5 for every customer overnight: the off-switch, realised. Portability across jurisdictions is the only mitigation, and it is available only on open standards, which is the deeper reason the green column on the next page matters.

None of this is an argument against proprietary software. You rent engines and runtimes, and that is normal. The argument is narrower, and it is about format: the authoritative copy of your meaning must sit on open standards you own, because every system downstream inherits the format of whatever is authoritative. Proprietary, platform-specific formats are fine as derived caches regenerated from that source; they must not be the source. Page 3 sets out the pattern.

Cap.	Capability	Open Agent Runtime	Hyperscaler			Enterprise Ecosystem	Data Cloud / Lakehouse	Knowledge Graph W3C / RDF	Property Graph
		OpenClaw, NemoClaw	AWS Neptune + Bedrock	Microsoft Fabric IQ, Copilot Studio	Google Vertex AI, Spanner Graph	SAP, ServiceNow	Databricks, Snowflake	Stardog, Graphwise, TopQuadrant, eccenca, metaphacts	Neo4j
9	**Agent Capability**	■ no governance	● Bedrock	● Copilot Studio	● Vertex AI	■	●	— (emerging)	—
8	**Agent Connectivity**	● MCP/A2A	■ MCP	■ MCP	● A2A	■	■ MCP	● MCP	—
7	**Provenance**	—	■ AgentCore	■ Purview	■ Agent ID	■	■	● PROV-O	—
6	**Guardrails**	—	■ AgentCore	■ Content Safety	■ Gateway	■	■	● SHACL	■ n10s post-hoc
5	**Agent Contracts**	—	■ AgentCore	■ Copilot Ctrl	■ Gateway	■	■	● ODRL/OWL	—
4	**Knowledge Graph**	—	● Neptune	■ Fabric IQ (prev)	■ Spanner	■	■	● SPARQL	■ Cypher
3	**Ontology**	—	● Neptune	■ Fabric IQ (prev)	■ Spanner Graph	■	■ catalog	● OWL/RDF	■ n10s (RDF import)

● On standards the organisation can own ■ Present but vendor-owned — Absent at the level required (preview) = not yet generally available

Key finding

What the marks measure is portability, not a brand of graph: the test is whether the organisation can own and move the standard, not whether it happens to be RDF. The dedicated knowledge-graph platforms (**Stardog**, **Graphwise**, **TopQuadrant**, **eccenca**, **metaphacts**) can cover Capabilities 3 through 8 on open standards the organisation owns. No other solution category provides equivalent coverage on portable standards. Hyperscalers, enterprise platforms, and data clouds provide functional governance on proprietary formats that cannot be exported or federated independently. Open agent runtimes cover L8–L9 but are absent at L3–L7 entirely.

The procurement question is not which vendor covers the most capabilities. It is which capabilities the organisation must own on standards it controls. The meaning capability (L3), the knowledge graph (L4), the agent contracts (L5), the guardrails (L6), and the provenance trail (L7) encode institutional knowledge and governance logic. Placing these on vendor-owned formats means rebuilding on every platform change.

Vendor notes

Microsoft. Fabric IQ, announced at Ignite in November 2025, is the hyperscaler investment most aligned with the Stack's meaning capability (L3–L4). Six months on, it remains in preview. Its ontology is a property-graph entity model, generated from a Power BI semantic model and queried in GQL, not an OWL ontology with SHACL and PROV-O. OneLake is open at storage, Delta and Iceberg, but the meaning capability is proprietary with no open export. The openness is at the lake; the ownership question is at the ontology.

SAP and ServiceNow. Both expanded governance offerings in May 2026. SAP introduced the AI Agent Hub on LeanIX at Sapphire 2026 (general availability Q3 2026, free with the Business AI Platform); ServiceNow expanded AI Control Tower at Knowledge 2026 with NVIDIA and Microsoft Agent 365 integrations. Coverage is functionally dense at L5–L7 in both cases, but the underlying meaning, on both sides, stays on vendor-owned stores.

Databricks and Snowflake. Both repositioned in 2026 as agentic-governance platforms: Agent Bricks governs agents through Unity Catalog, Cortex Agents through Horizon Context. In each case the meaning lives in a catalogue and a semantic-views layer, exposed to agents over MCP, not an OWL ontology with SHACL and PROV-O on open standards. That is functional governance the organisation rents, not a meaning capability it owns; both also back the Open Semantic Interchange, with the same caveat as the watch signal below.

Amazon. Neptune Analytics can import open-standard graphs but stores and runs them in its own property-graph form, so the version that actually operates is vendor-defined. Convergence at the surface does not change the ownership question underneath.

Neo4j and property-graph platforms. A property graph is a graph, not by itself a meaning capability. It stores entities and relationships with local identifiers and enforces basic constraints, but the formal definitions, rules, and provenance that let meaning be validated and carried between systems are added in application code rather than authored as portable, open-standard artefacts. These platforms can be extended toward semantics and are strong operational graphs; the ownership question is whether the meaning is the organisation's to move, or the vendor's to hold.

Palantir. Managed deployment platforms (Palantir AIP with Forward Deployed Engineers) can cover L3–L9 comprehensively as a proprietary service. They sit outside this diagnostic because their delivery model differs structurally from software platforms an organisation operates itself.

Watch signals for Q3

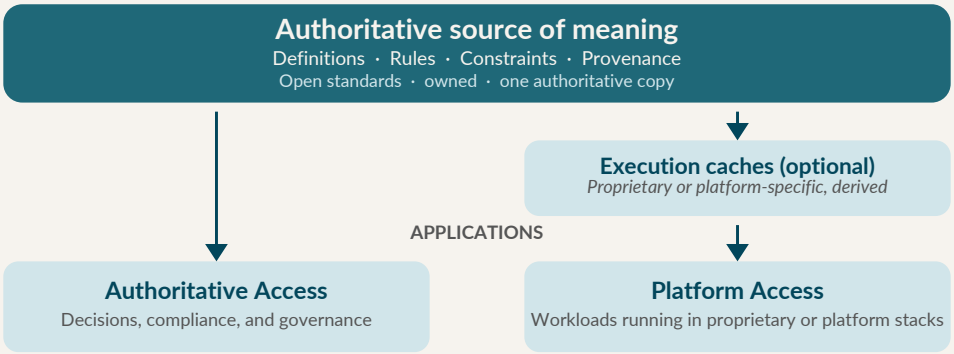
RDF 1.2. A new version of the core open standard reached a near-final stage in April 2026. The signal to watch is vendor support: once two or more major graph engines ship it, the main remaining technical objection to running open standards for live workloads falls away, and any decision to commit to a single vendor's proprietary graph format deserves revisiting.

Open Semantic Interchange. ServiceNow joined the OSI in June 2026. It moves no cell: the Diagnostic scores shipped coverage, not membership, and OSI standardises how metrics and definitions are exchanged, not the reasoning, rule-checking, and audit the governance capabilities depend on, so ServiceNow's amber marks at L3 to L5 hold. The signal to watch is whether OSI's working group maps its concepts onto the open meaning standards in this stack, a bridge to the open capability, or onto a simpler format without formal meaning, a parallel format beside it. The former would strengthen the case here.

Canonical reference: The Agentic AI Capability Stack™, Version 3.1. Based on publicly available information, Q2 2026. Not independent audit. The Diagnostic assesses coverage and ownership on open standards, not performance; vendor performance benchmarks should be validated against organisational workloads. Licensed CC BY-ND 4.0 with attribution.

One authoritative source, two access paths

Authority stays in the meaning capability. Everything else is derived from it.



The access path is a choice of risk and fit, not a limit of the source.

The recommended pattern keeps one authoritative source on open standards the organisation owns: the canonical definitions, rules, and audit trail. Where a proprietary or platform stack already runs the work, the organisation derives an execution cache from that source rather than authoring the meaning twice. Applications read directly from the meaning capability for decisions that carry risk, compliance, or governance weight, and through a derived cache where the work runs inside a proprietary stack.

A cache earns its place only when the organisation can replace it, or change the stack beneath it, and regenerate an equivalent without losing meaning, rules, or audit. Authority never moves into the cache. That line, what is authoritative and what is derived, separates using a proprietary stack from depending on one.

The pattern is in production. Netflix's Unified Data Architecture holds one authoritative model on open standards and projects it into every representation its platforms need; its own name for the principle is “model once, represent everywhere”.

The coverage matrix on page 2 reads directly through this pattern. A green mark identifies a store that can hold the authoritative copy, on standards the organisation owns. An amber mark identifies a legitimate execution cache: usable, often valuable, never the place the meaning is defined. The matrix is therefore a map of what may be cached and what must be owned.

Six contract tests

The pattern becomes enforceable when it is written into vendor contracts. Articles 3a to 3c of the series derive six criteria that function as deal-stoppers in platform evaluation:

Test	What the contract must guarantee	Sovereignty protected
1. Configurability	Governance rules are client-configurable without a vendor software release	Enforcement
2. Enforcement timing	Runtime enforcement fires before execution, not as logging after the fact	Enforcement
3. Portability	The meaning capability sits on open standards, portable across platforms	Semantic
4. Provenance	Every agent decision links, at the moment of action, to the governance framework in force at that time	Semantic
5. Verifiable execution	The runtime produces evidence the agent ran as specified, independent of the infrastructure provider’s word	Execution
6. Jurisdictional continuity	If a government compels the provider to cut access, through sanctions or export control, the organisation can keep the governed stack running from exports it already holds, on infrastructure or in a jurisdiction it controls, without the provider’s cooperation	Jurisdictional

Any one absent, and the corresponding sovereignty rests with the vendor regardless of the organisational chart.

Where common terms sit

MCP and A2A are connectivity protocols at Capability 8: they standardise how agents reach tools and governance, not what the governance says. **GraphRAG** is a retrieval pattern that reads from the knowledge graph (Capability 4) to improve answers; it consumes the meaning capability and is not a substitute for owning it. **BI semantic layers** define metrics and dimensions for human analytics. They draw on the data foundation (Capabilities 1 to 2) and run parallel to the stack, not within it; they are not the meaning capability (Capability 3) an agent is governed against. BI is not agentic AI.