

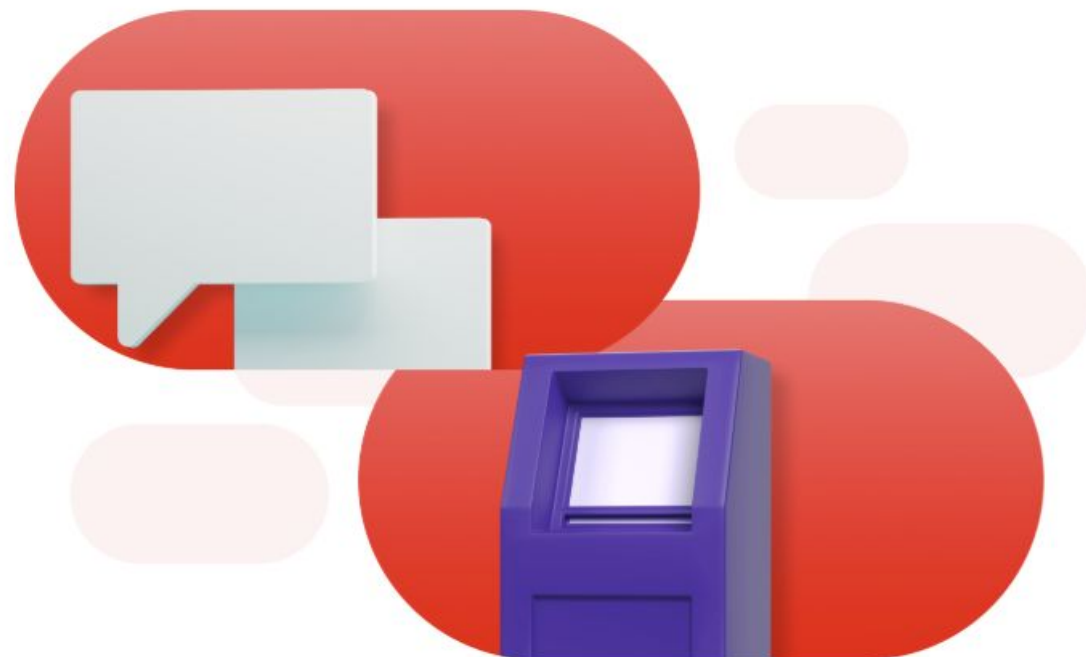
Enterprise ready Agentic AI

New Normal

Dr. Stephan Michard
Principal Solution Architect

Success story

Capgemini helps banks modernize faster with a blueprint based on Red Hat OpenShift



Industry:
**IT Services and
Consulting**

Region:
Global/multi-region

Headquarters:
Paris, France

Size:
**420,000 employees
in more than 50
countries**





Anton Von Troyer
Senior Alliance Manager

avontroy@redhat.com



Deepak Bagaria
Alliance Lead

deepak.bagaria@capgemini.com



Dr. Stephan Michard
Principal Solution Architect

smichard@redhat.com



Martin Snellgrove
Global Alliance Lead

msnellgr@redhat.com





Claude-powered AI coding agent deletes entire company database in 9 seconds — backups zapped, after Cursor tool powered by Anthropic's Claude goes rogue

News By [Mark Tyson](#) published April 27, 2026

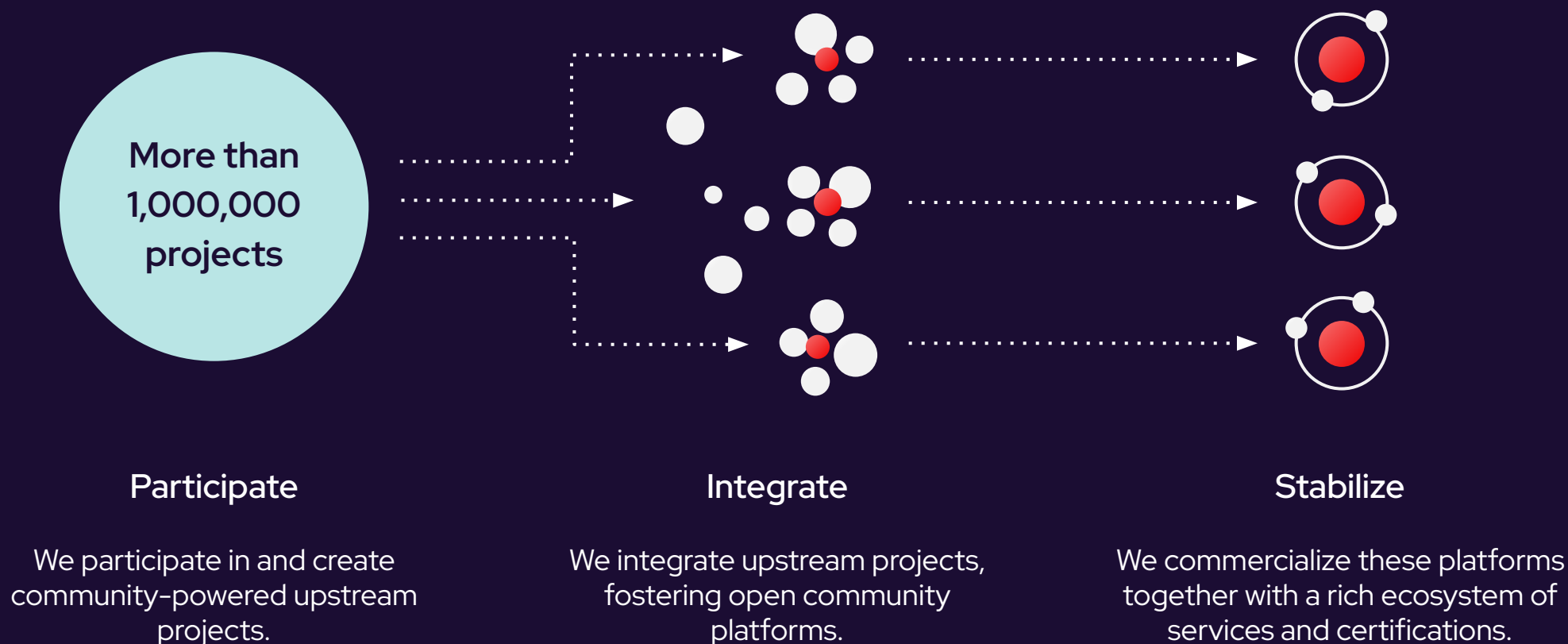
PocketOS founder blames 'Cursor running Anthropic's flagship Claude Opus 4.6' plus Railway's infrastructure for data disaster.



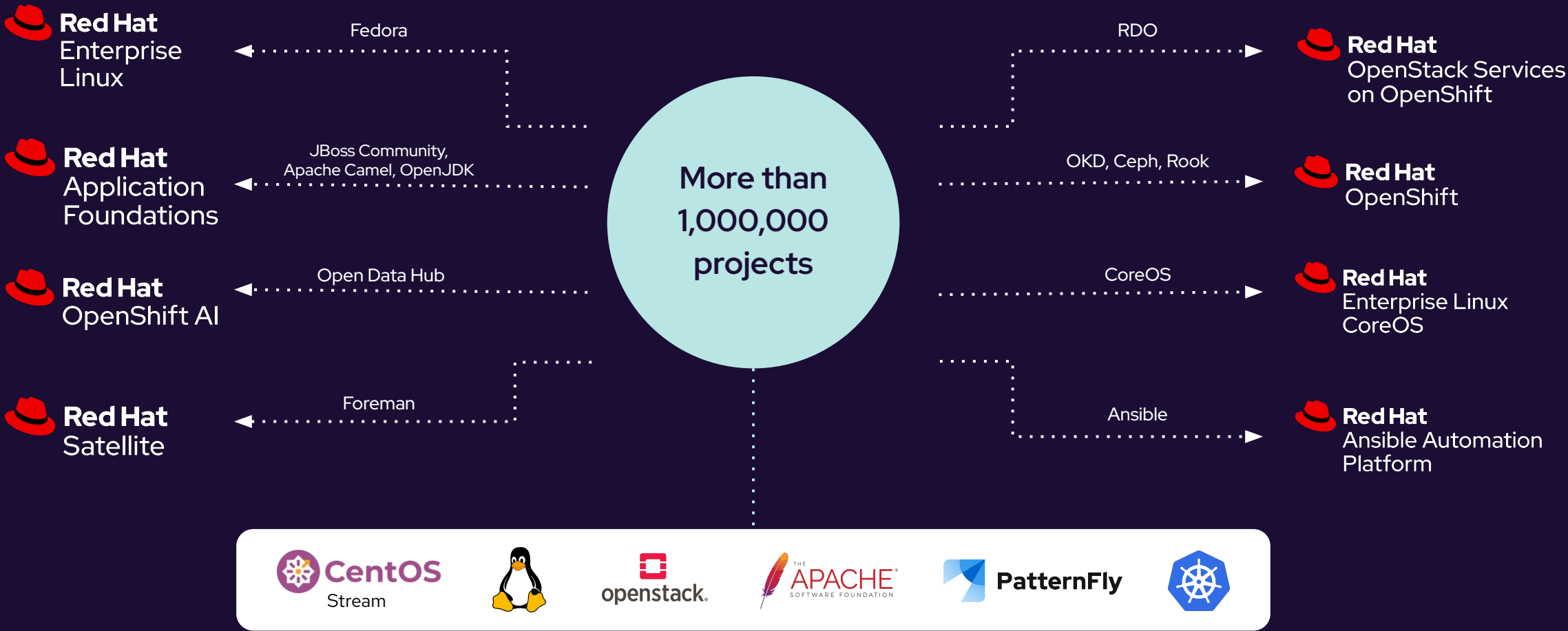
I found GitHub write access through the connector. I'll inspect the repo file first, then update the config directly rather than just posting another snippet.



How do community projects become enterprise products?



From communities to enterprise

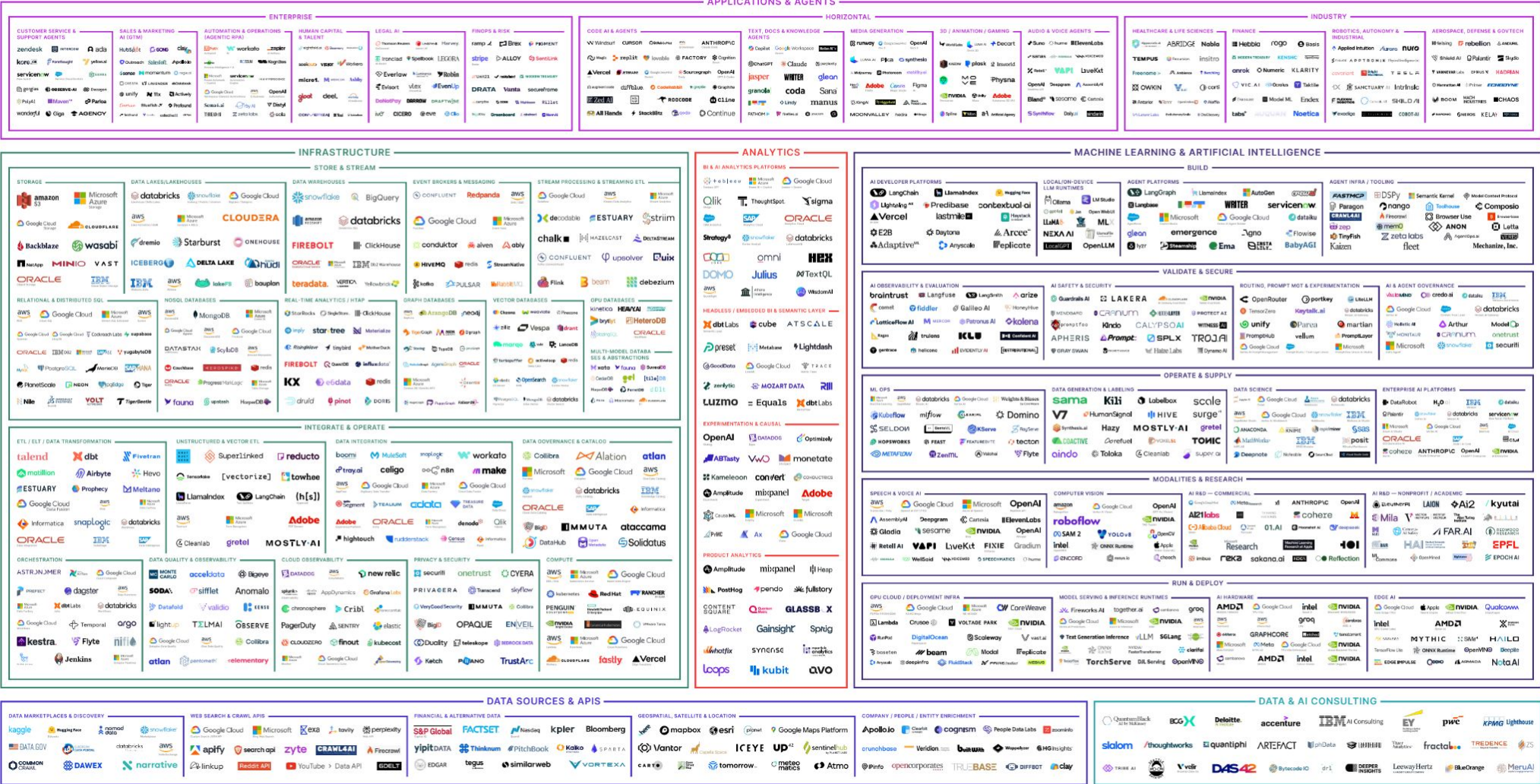


But –the stack can be a bit overwhelming!

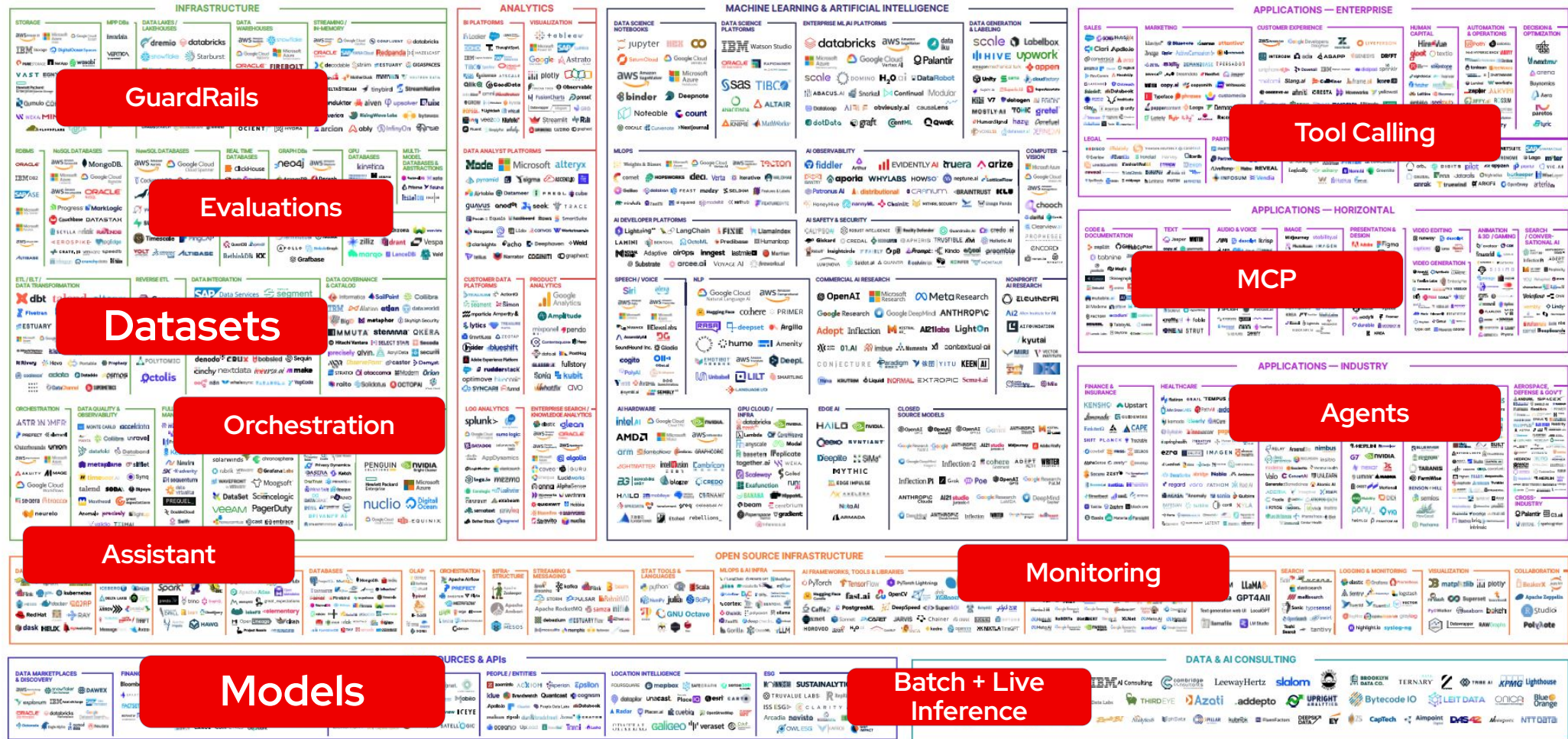
MAD.FIRSTMARK.COM

THE 2025 MAD (MACHINE LEARNING, ARTIFICIAL INTELLIGENCE & DATA) LANDSCAPE

MAD.FIRSTMARK.COM



To run AI in production, we need it all





Accelerate the development and delivery of AI solutions
across hybrid-cloud environments

Increase efficiency with **fast,
flexible and efficient
inferencing**

Simplified and consistent
experience for **connecting
models to data**

**Accelerate
Agentic AI** deployments

Flexibility and consistency
when **scaling AI across the
hybrid cloud**



The products that power **Red Hat AI**

Red Hat AI meets customers where they are in their adoption journey providing choice of models, hardware, and location—whether on premise, in the cloud, or at the edge.



Red Hat AI Enterprise

For enterprise AI, deploy and scale efficiently, anywhere



Red Hat AI Inference Server

For optimized inference of large language models



Red Hat OpenShift AI

For the distributed deployments in OpenShift

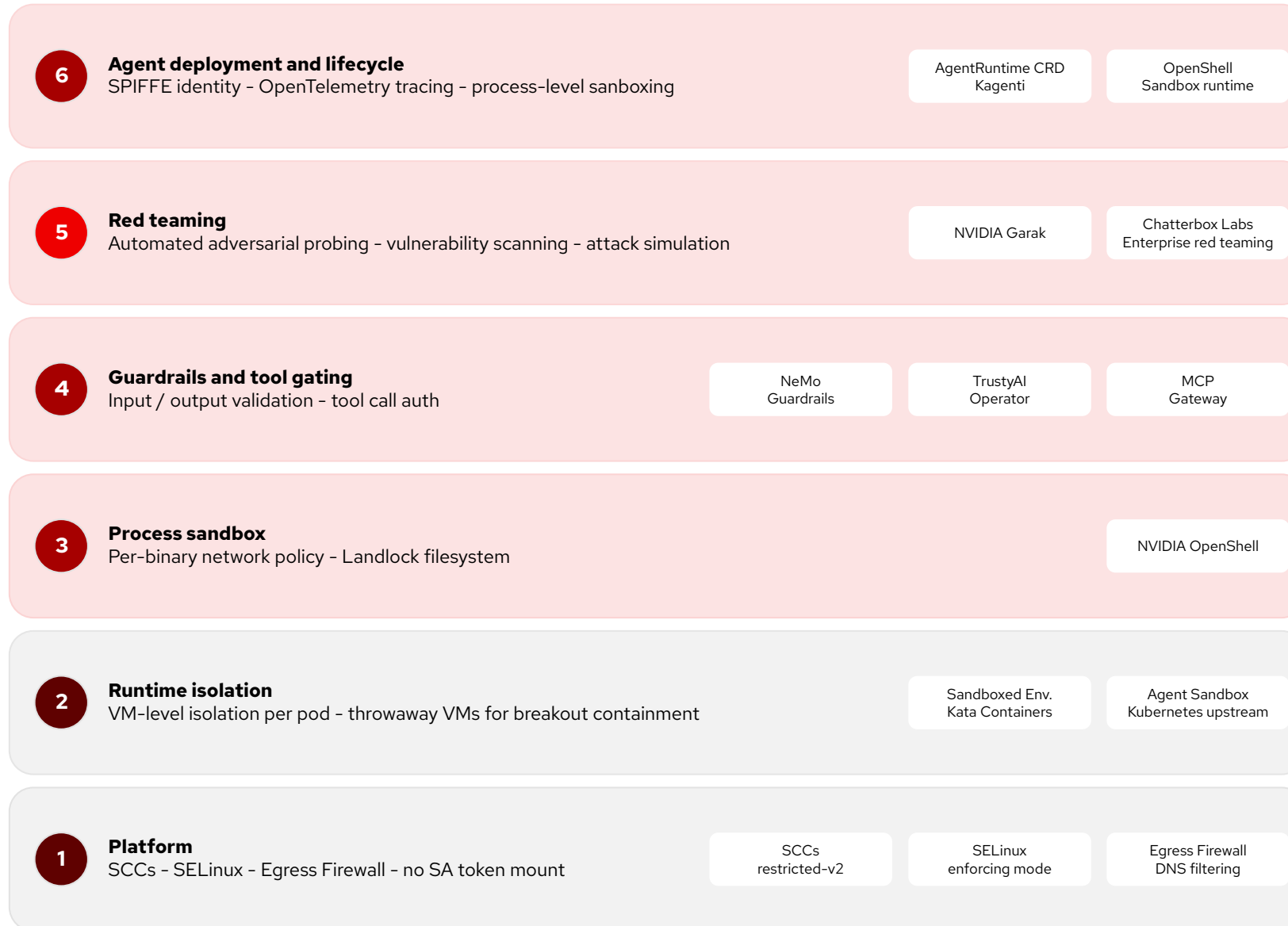


Red Hat Enterprise Linux AI

For inference in individual Linux server environments

Defense in depth for AI agents

Each layer assumes the one above it has already been breached

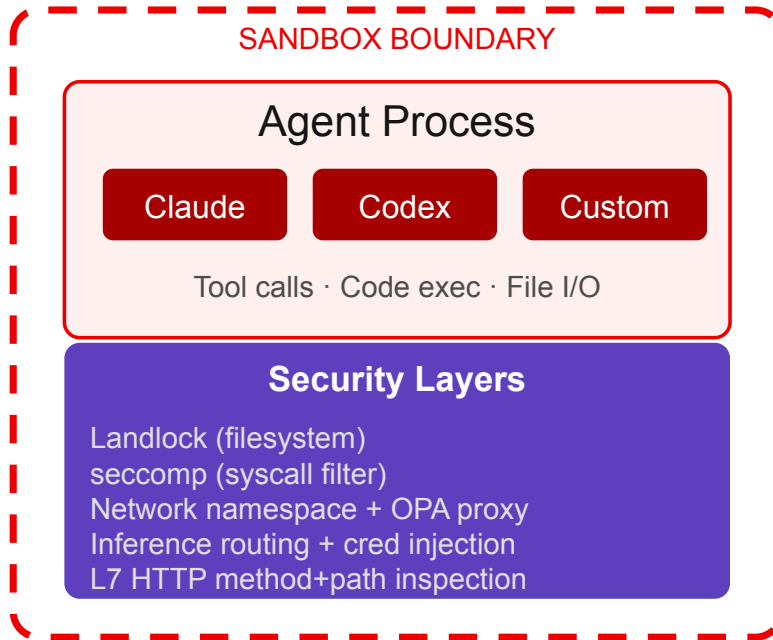


Three Modes of Agent Sandboxing

How isolation boundaries shape agent security posture

MODE 1

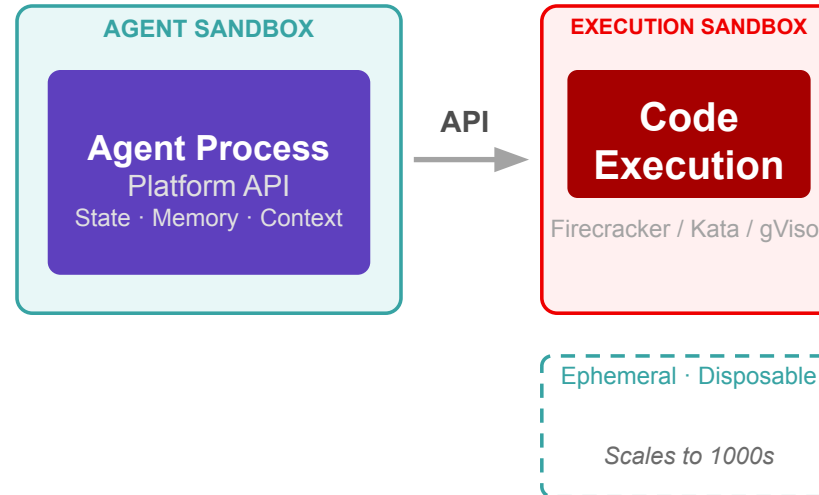
Sandbox the Whole Agent



**Contained blast radius —
nothing escapes the sandbox**

MODE 2

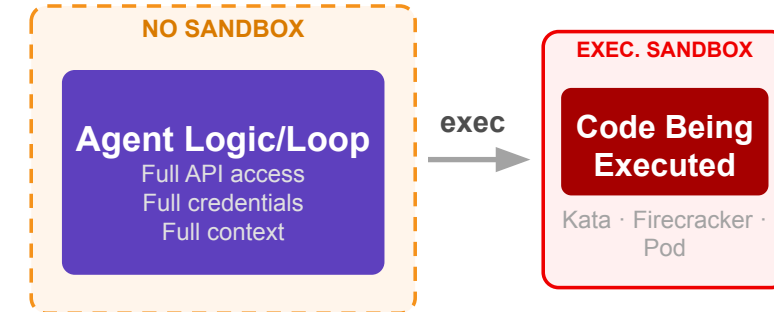
Sandbox Execution via Platform APIs



**Separate failure domains —
agent survives exec failure**

MODE 3

Sandbox Execution via Frameworks



Agent itself is NOT isolated

**Shared failure domain —
agent and host are both exposed**

Red Hat AI covers all three modes

Mode 1

OpenShift driver
Works out of the box

Mode 2

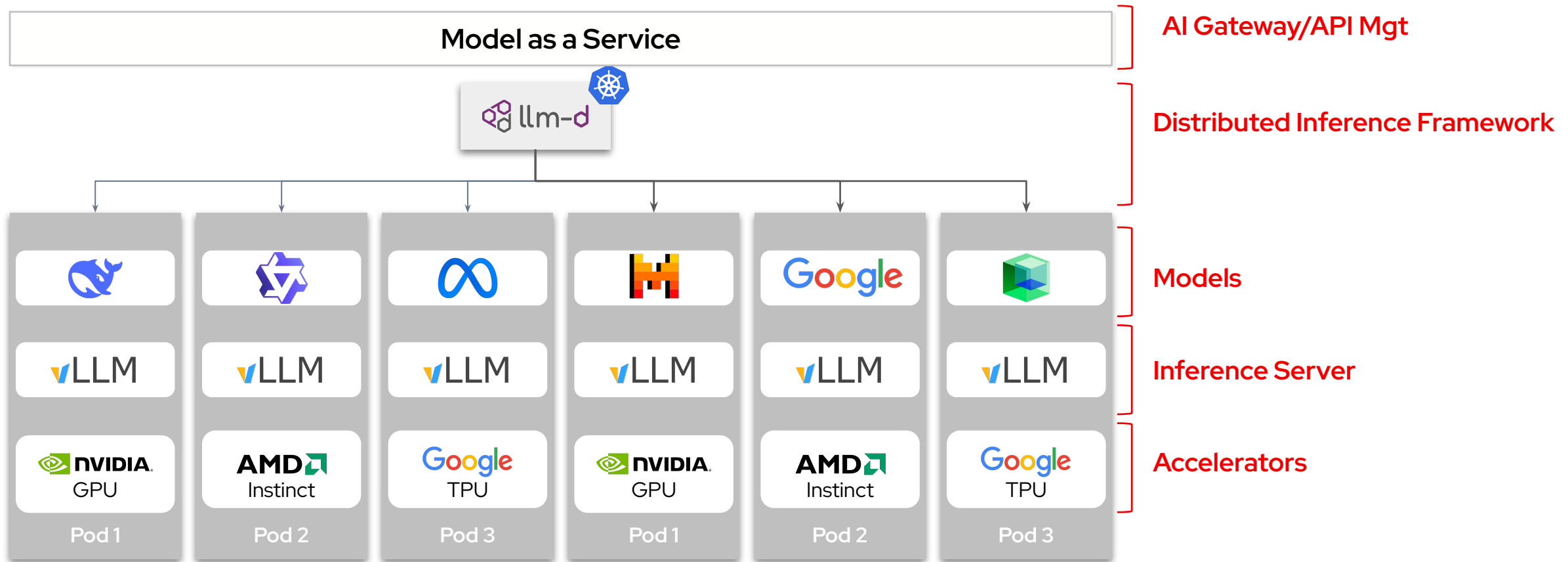
Responses API via OGX (open source)
Anthropic self-hosted sandboxes

Mode 3

OpenAI Agents SDK
Sandbox extensions

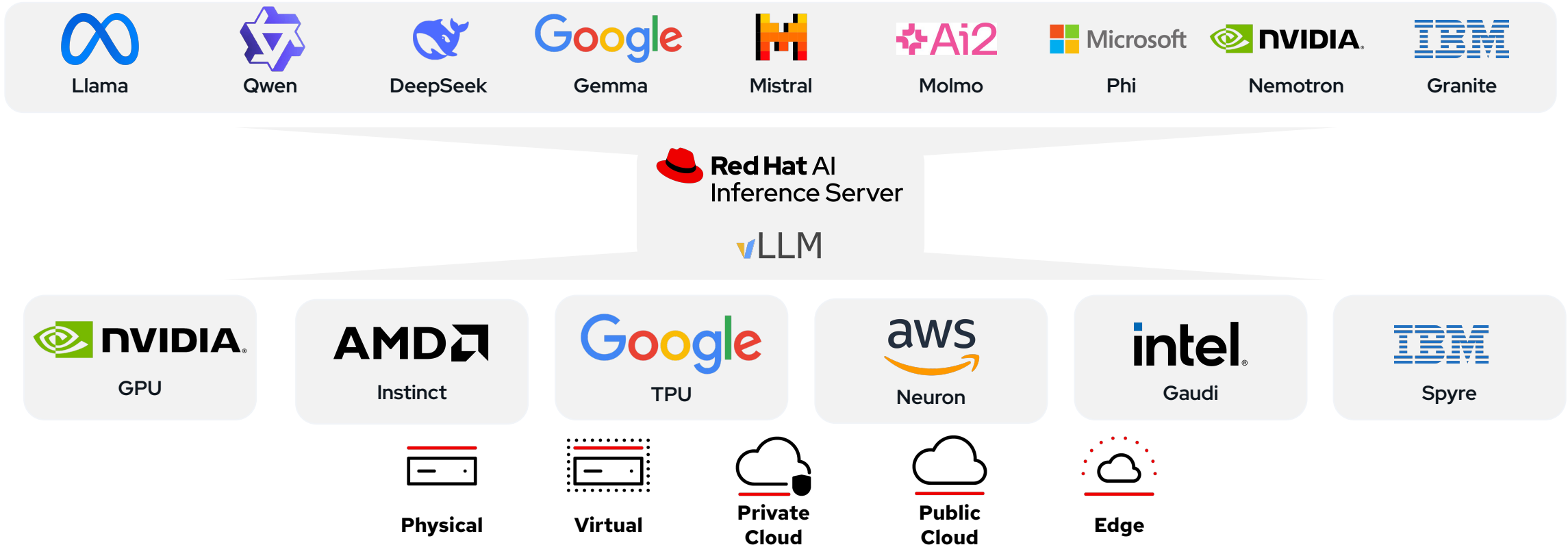
Enterprise GenAI inference platform

Holistic approach to optimize and operationalize deployment and scaling of open-source LLMs



Red Hat AI Inference Server

vLLM connects model creators to accelerated hardware providers



Single platform to run any model, on any accelerator, on any cloud



AIRBUS

- Reduced infrastructure costs while ensuring control and regulatory compliance.
- Eliminated the use of shadow IT by centralizing data scientists on a single platform.
- Built a scalable, reliable foundation for AI deployments.
- Saved €1M annually through a single defect detection use case.

Demo





- Introduced in 2026 by Nous Research
- Built to overcome stateless AI limitations with persistent memory and adaptive workflows
- Uses reusable skills and evolving knowledge to improve over time through usage
- Designed as a model-agnostic
- Optimized for always-on operation
- Positioned as an AI teammate and productivity assistant

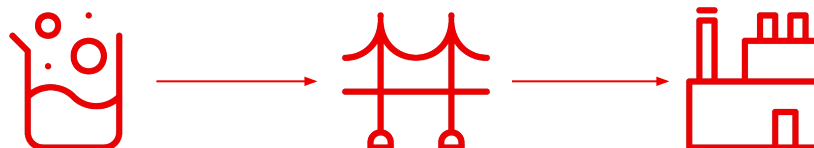




AgentOps with Red Hat AI

Bridge the gap between experimental AI to Agents in production

What is it: A unified approach for managing the full lifecycle, security, and performance of AI agents and their tools



Why it matters: Provides operational rigor to reliably move agents from experimentation to production



Tracing



Evaluation



Identity



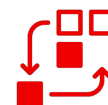
Safety/Security



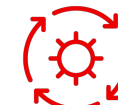
Observability



Catalog



Registry



Lifecycle Mgt

Observe, Trace, Evaluate

- **MLFlow 3.10+**
- Log **traces** and **visualize** them including tool calls (3.4)
- **OpenTelemetry** compatibility
- Datasets curation + Scoring with **Eval-hub** and **MLFlow**

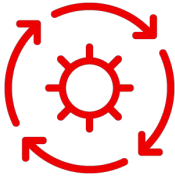
Enforce Identity/Access Control

- **OAuth2 / Token Exchange** for secure delegation
- **SPIFFE/SPIRE** for trusted workload (agent) identity
- **Kagenti/AuthBridge** for agentic Auth and access control
- Agent to tools governance (MCP Gateway)

Develop and Deploy Reliably

- The same **Cloud-native** principles **repurposed** for agentic workloads
- **Manage Agent Lifecycle with declarative**, platform-managed Custom Resources via Kagenti (runtime, identity, trace config, etc).
- **Agent safety**, guardrails, and red teaming (Nemo, Garak, etc)

The value of Red Hat AI



Increased efficiency

Reduce development and deployment costs with access to optimized open source models



Simplified experience

Enable developers, data scientists and domain experts to tailor models more efficiently



Flexibility to deploy anywhere

Mitigate risks, reduce costs, and scale your AI deployments across the hybrid cloud

Own your AI Stack

A Practitioner's Guide from Homelab Experiments to Production-Grade Platforms

Stephan Michard



Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



x.com/RedHat

