

INTELLIGENCE // CONNECTIVITY // INNOVATION

A complete, private AI workforce **in a box** — installed in your office, owned by you.

Everyone else rents you intelligence over the wire and keeps your data. The **Omniscient Core** is a hyper-secure appliance installed on your premises — preloaded with a hardened OS, local AI models, a fleet of agents, every Claude skill you use today, and an open-source equivalent of nearly every business application, all pre-integrated so the AI doesn't just chat, it acts. And it compounds: an enduring knowledge graph for every department and employee (so institutional knowledge survives staff turnover), plus self-improving workflows that get cheaper and faster every run. We don't prompt the AI — we allocate skills to tasks and let efficient loops optimise themselves.

COST

Lease, not per-seat

3-year lease + local inference — fully R&D-claimable. Marginal cost of a query ≈ electricity. Unlimited seats & agents.

PRIVACY

Data never leaves

On-prem, single-tenant, air-gapped. No inbound internet path. Nothing leaves without a logged human approval.

FLEXIBILITY

Your guardrails

Customer-owned, customer-tuned open-weight models. No foreign safety desk blocking specialist work.

COMPLIANCE

AU by design

Onshore by physics. Built to support the Privacy Act & AU AI guardrails, kept current by subscription.

■ The security a CISO actually asks about

“Can our data leave?”

No inbound internet path, ever. A single default-deny egress broker permits only two pinned destinations — consented burst and signed updates. One switch → island.

“Can the AI go rogue once it's wired into everything?”

Agents can't call tools directly. A policy broker gates every action; anything consequential (money, PII, sends, deletions) needs human or dual approval. Injected instructions are tainted and can't escalate.

“Is there a backdoor for Omniscient?”

No standing access. Support is customer-initiated, time-boxed, recorded to your ledger. You hold the recovery keys; our escrow share can't decrypt alone.

“How is it updated without one?”

The box pulls signed updates — no push, no open port — verifies and applies them with auto-rollback, in windows you approve. Compliance updates arrive the same trusted way.

■ What's inside the box

GOVERN

Tamper-evident audit ledger — every action provable

AGENTS

Pre-built agents & workflows, wired to your apps

SOFTWARE

Open-source CRM · ERP · BI · docs · comms

AI

Local open-weight models + opt-in consented burst

OS

Immutable, signed, self-healing hardened Linux

HARDWARE

AMD/Intel · 128–256GB · 48GB+ GPU · NVMe + NAS, right-sized · compact→rack

Mid-market ready. Business tier targets 99.5% availability; HA upgrade reaches 99.9%+. Operational-metrics-only telemetry, opt-out — proactive support without ever touching your content.

“We hand you an AI workforce that's **yours to command** — never rented over the wire, never leaving the building. And it **proves it.**”

[Book a sovereignty briefing →](#)
omniscientai.io · enquiries@omniscientai.io
Melbourne · vendor-neutral · Australian-sovereign