Diagnara

From outage to root cause in minutes.

Evidence-driven AI for enterprise incident investigation. Diagnara runs governed, multi-agent investigations across your logs, metrics, deployments, tickets, databases and business systems — and returns conclusions backed by traceable evidence, not chat summary.

- EVIDENCE-DRIVEN
- BUSINESS CONTEXT
- PROTOCOL OVER IMPROVISATION
- GOVERNED BY DEFAULT
- AUDITABLE

OBJECTIVE

Diagnara reduces MTTR and improves operational efficiency — through autonomous, evidence-driven incident investigation.

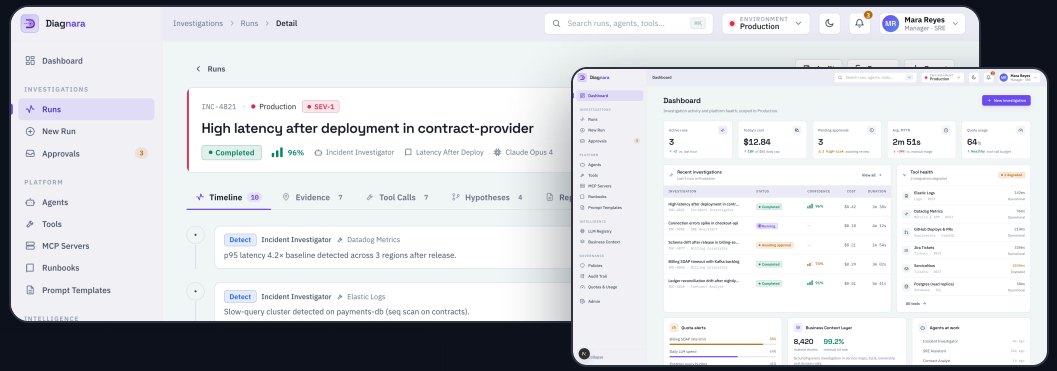
Mean Time To Recovery is the metric Diagnara is built to move. Every capability that follows exists to find the root cause faster, with proof.

Incident response in financial services is manual correlation against the clock.

Today, during an incident

- **Evidence is fragmented** across observability tools, tickets, deployment history, databases, billing and payment systems — each behind a different team.
- **Engineers correlate by hand**, against the clock, while a payment window, reconciliation batch or SLA deadline keeps running.
- **Existing tools watch one system at a time** — they don't correlate across systems and have no business context layer to judge what a signal means.
- **Generic AI tools summarize** — they don't investigate. Their answers carry no defensible justification for engineering, compliance or audit.
- **Knowledge evaporates** after each incident: the next on-call engineer starts from zero.

With Diagnara



The Diagnara Console: a real investigation — timeline with approval gates, cited evidence, tool calls, tested hypotheses and an audit-ready report. Structured investigations grounded in your business context — not a chatbot.

THE EVIDENCE PIPELINE

01 — Detect
Alerts, tickets or manual prompts trigger an investigation.

→

02 — Investigate
Multiple sources are validated and weighed against your business domain.

→

03 — Correlate
Evidence gathered and compared across governed systems.

→

04 — Conclude
Root-cause hypothesis with confidence, impact and next actions.

→

05 — Institutionalize
Timeline and evidence stored for reuse on future incidents.

Other tools look at one system. Diagnara sees the whole ecosystem.

PROBLEMS WITH OTHER TOOLS

- **No correlation across systems** — each tool sees its own silo.
- **One layer only** — logs *or* source code *or* deployments.
- **No business context** to judge what a signal actually means.

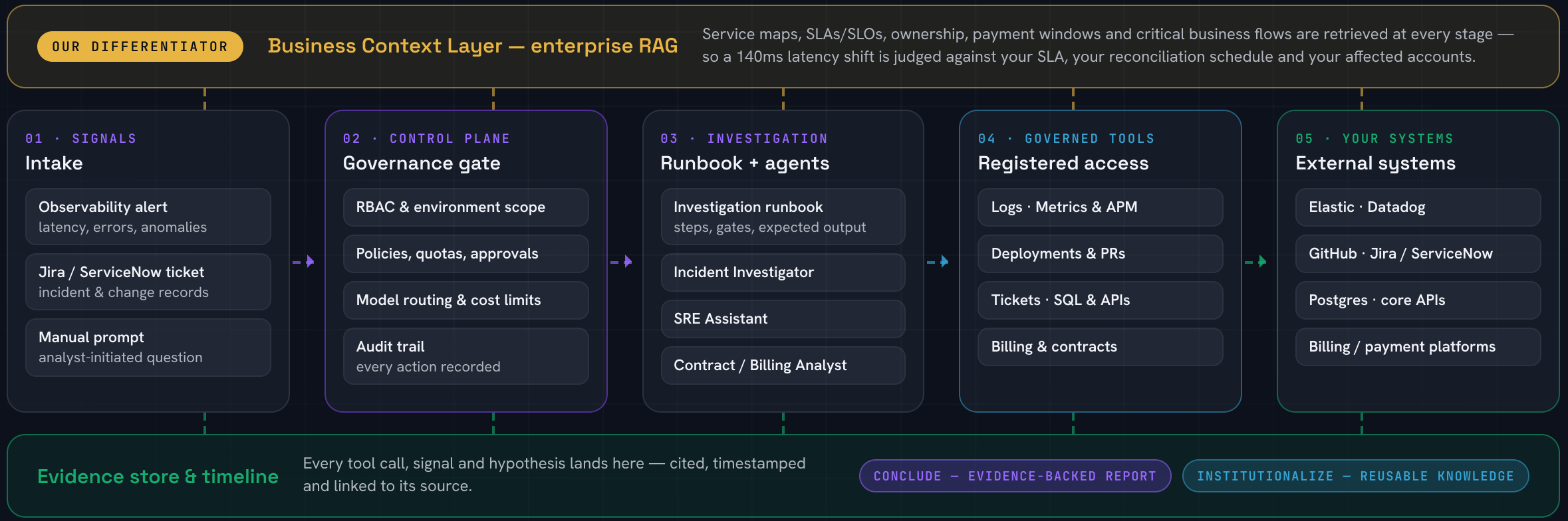
THE DIAGNARA APPROACH

A macro view of the entire ecosystem.

- Correlates **source code, APIs, data, AWS infrastructure, deployments and logs** in a single investigation.
- **Business Context Layer** — the key differentiator — judges signals against your reality.
- Reasons over **system interactions**, not isolated metrics.

How a signal becomes an evidence-backed root cause.

Every investigation flows through a governed control plane before any agent touches a system. Access, policy and audit are enforced on every step.



04 — GOVERNANCE

Constrained and controlled — unlike a generic copilot.

Compared to traditional copilots, Diagnara **does not run freely**. It operates inside a customized MCP with explicit limits.

01	**Token consumption monitoring**	Every run's model usage is measured and capped — predictable cost, no runaway spend.
02	**Cost efficiency by design**	Right-sized LLMs, well-targeted prompts and procedural workflows keep token usage — and cost — low.
03	**Read-only access**	The MCP is configured for read-only — Diagnara observes and reasons, it never changes your systems.
04	**Safer execution**	Tools are constrained to investigation only — no open-ended actions, no improvisation.
05	**Full auditability**	Every signal, tool call and hypothesis is recorded — the whole investigation is on the record.

Read-only access, deployed inside your environment.

READ-ONLY PERMISSIONS

- **GitHub** — source code & recent changes.
- **AWS** — infrastructure status.
- **ServiceNow** — incident data.
- **New Relic** — logs, read at investigation time.

No write access — ever

Nothing leaves your scope

DEPLOYMENT & USAGE

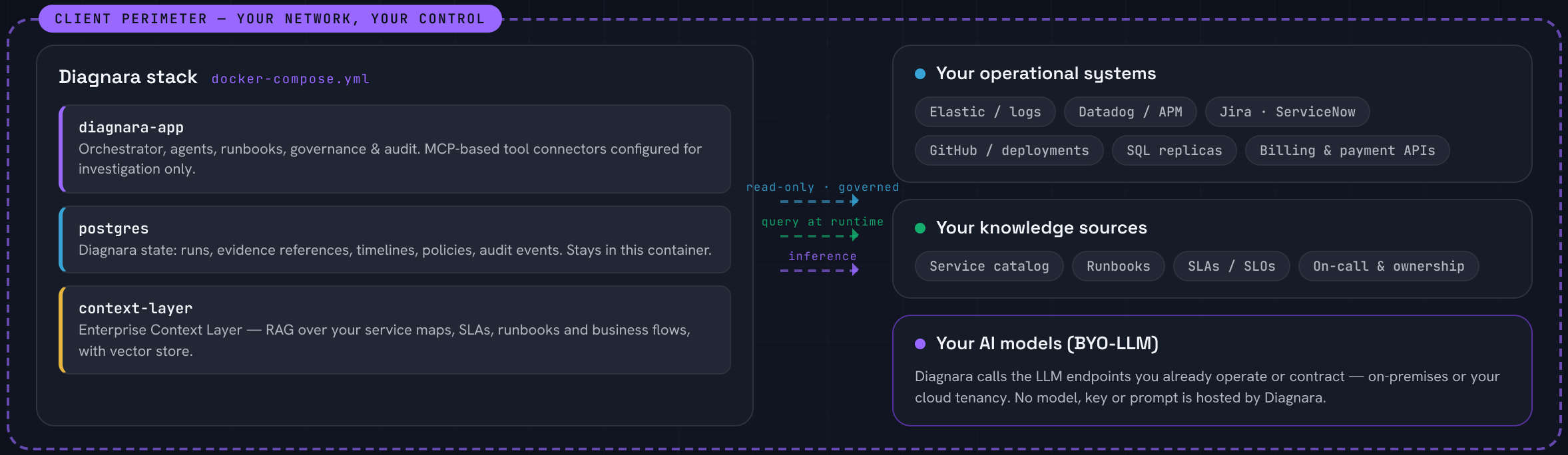
- **Local Docker container** inside your environment.
- **No additional infrastructure** to provision.
- **Fully isolated** — stays within your perimeter.
- **Free during the pilot** — no licence cost.

SECURITY & COMPLIANCE COMMITMENTS

- ✓ **BYO-LLM.** Inference runs on the client's own AI models and endpoints.
- ✓ **Zero log retention.** Raw log data is read at investigation time, never stored.
- ✓ **Data residency.** No client information leaves the client's scope or network.
- ✓ **Free to use.** The pilot — and the tool — carry no licence cost.
- ✓ **GDPR-aligned.** No personal data is transferred to or processed by Diagnara.
- ✓ **Your IP stays yours.** Client data, prompts and derived knowledge remain client property.

Deployed inside your perimeter. Nothing leaves your network.

Diagnara ships as a docker-compose stack on infrastructure you control. It connects to your systems and your AI models — there is no Diagnara cloud in the data path.



Zero egress by design. All connections are outbound from the Diagnara stack to systems inside your perimeter. Diagnara stores references and conclusions — raw log data is read at investigation time and never retained.

Measurable impact for engineering and operations leadership.

Operational efficiency

- **Reduce MTTR** — mean time to recovery
- **Less downtime** on critical systems
- **Less customer impact** during incidents

Engineering productivity

- **Less effort** for engineers during investigation
- **Faster root-cause identification**
- **Fewer escalations** — first-line teams resolve with evidence

Diagnostic quality

- **More precise**, evidence-based diagnostics
- Grounded in the **Business Context Layer**
- **Beyond logs** — code, APIs, data & deployments

Governance & security

- **Full auditability** — every step on the record
- **Token monitoring** — predictable cost
- **Read-only MCP** — scoped to investigation, safe by design

FINAL STATEMENT

Shift from reactive monitoring to Autonomous Incident Investigation.

Start the conversation

Marcos Agostta — Founder & CEO

linkedin.com/in/marcos-agostta

www.diagnara.com

www.diagnara.com/documentation