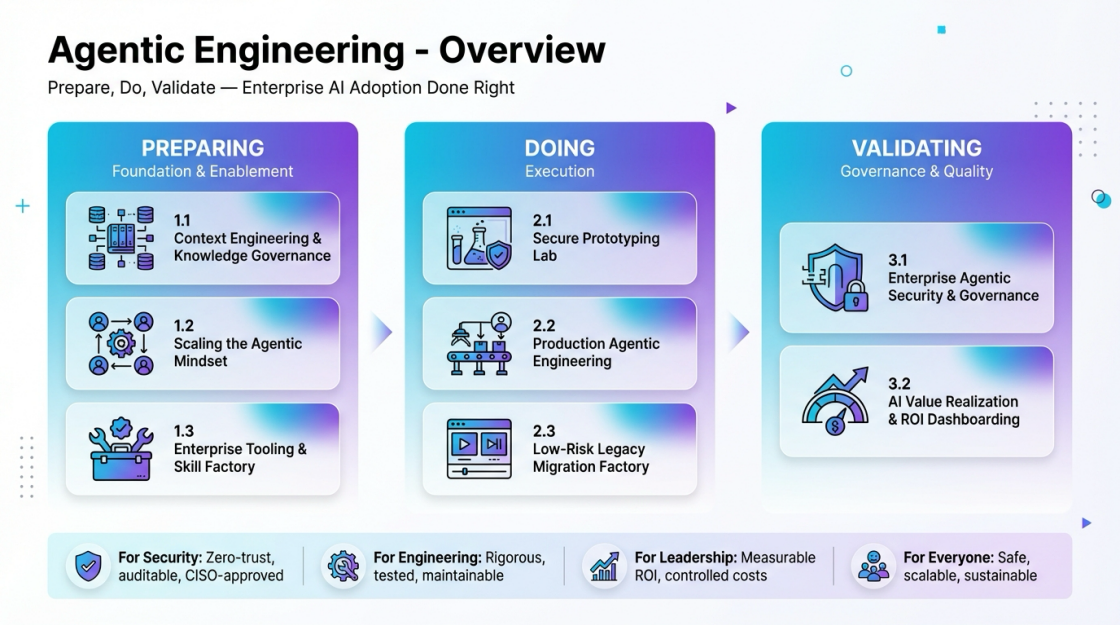
Agentic Engineering Consulting Offerings

Prepare, Do, Validate — Enterprise AI Adoption Done Right



Why this exists

Most organisations are stuck between two realities:

- A handful of champions are getting real leverage from tools like Claude Code.
- Security, IT, and leadership can't approve a rollout without controls, repeatability, and proof.

This brochure describes eight offerings that turn "agent experimentation" into a safe, scalable, measurable capability.

How to read the portfolio

The offerings follow a simple maturity path:

1. **Preparing** — make behaviour predictable (rules, knowledge, people, tools)
2. **Doing** — deliver outcomes safely (prototype, build, migrate)
3. **Validating** — keep risk down and value visible (security, governance, ROI)

The Offerings

1.1 Context Engineering & Knowledge Governance

What it is
A “single source of truth” for agents: **Hot Rules** (always-on governance) + **Cold Knowledge** (curated reference), with ongoing **context hygiene**.

What you get
- Global rules and policy packs (coding standards, security constraints, “how we work”) - Usage specs + golden paths for internal libraries and platforms - Automated discovery + maintenance approach (preventing “context rot”)

Best for
Platform/architecture leaders, security advocates, and teams who need consistent outcomes across many developers.

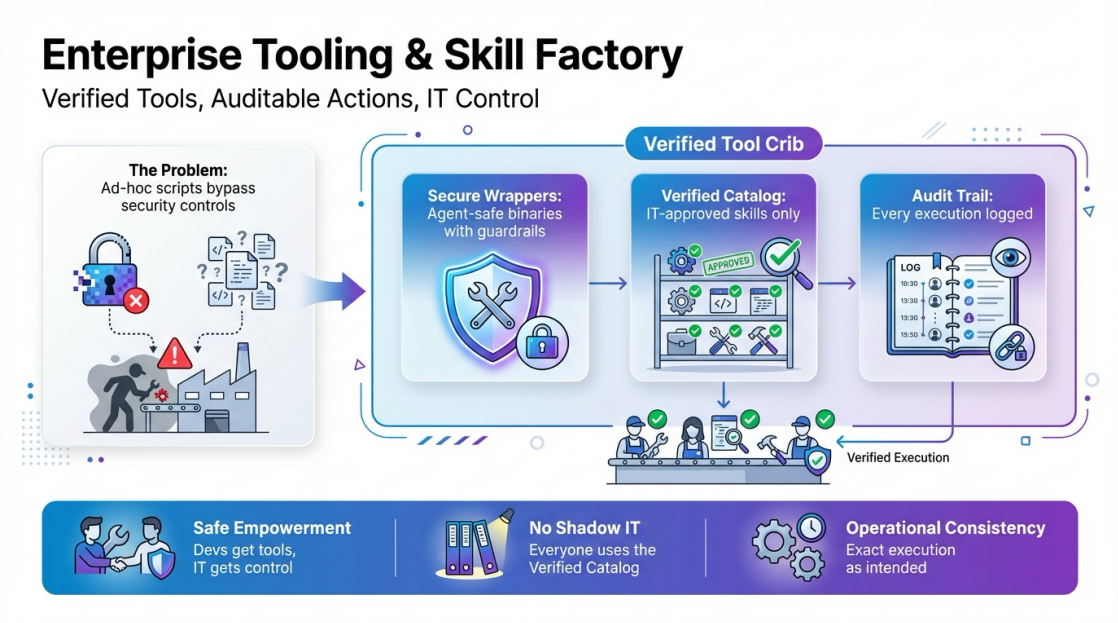
1.2 Scaling the Agentic Mindset

What it is
A scalable operating model for working with agents: **RIPER** (Research → Innovate → Plan → Execute → Review) plus train-the-trainer enablement.

What you get
- A lightweight SOP for engineers, reviewers, and managers - Champion programme design and internal enablement materials - Review and quality practices that prevent “acceptance fatigue”

Best for
Teams moving from a champion-led pilot to broad adoption without quality collapse.

1.3 Enterprise Tooling & Skill Factory

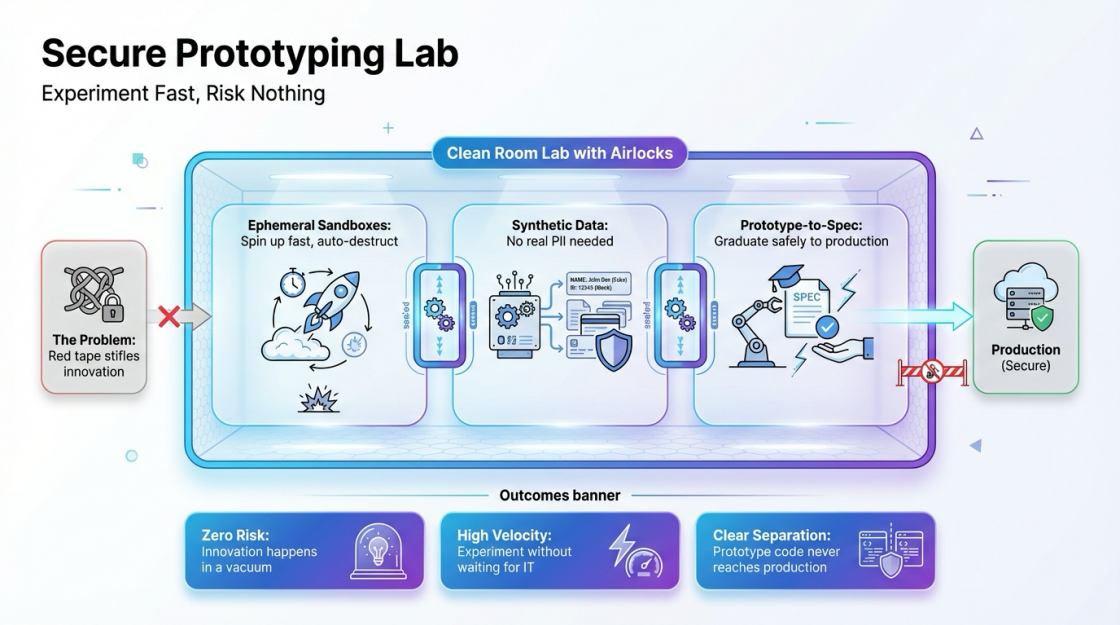


What it is
A controlled way to give agents power: build **verified skills** instead of ad-hoc scripts, with auditability and permission gating.

What you get
- A verified catalog of agent tools/skills (approved actions only) - Safe wrappers for high-risk operations (confirmations, least privilege, logging) - Operational handover: ownership model, maintenance, and governance

Best for
Engineering CoEs, DevTools, and IT/security teams that need “fast for champions, safe for the enterprise”.

2.1 Secure Prototyping Lab

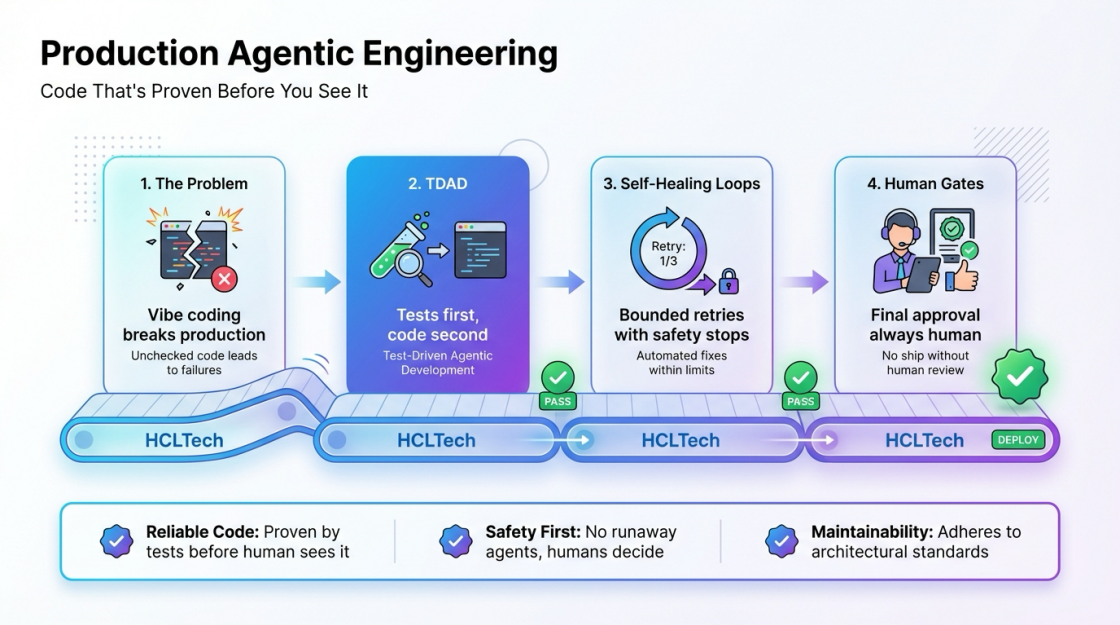


What it is
A fast, safe way to move from idea to prototype using agents without touching production systems or sensitive data.

What you get
- Ephemeral sandbox environments (isolated; no host OS access) - Synthetic data patterns so teams can build credible demos safely - Prototype-to-spec handover to graduate learnings into production engineering

Best for
Innovation teams and Engineering CoEs proving value quickly without creating hidden risk.

2.2 Production Agentic Engineering

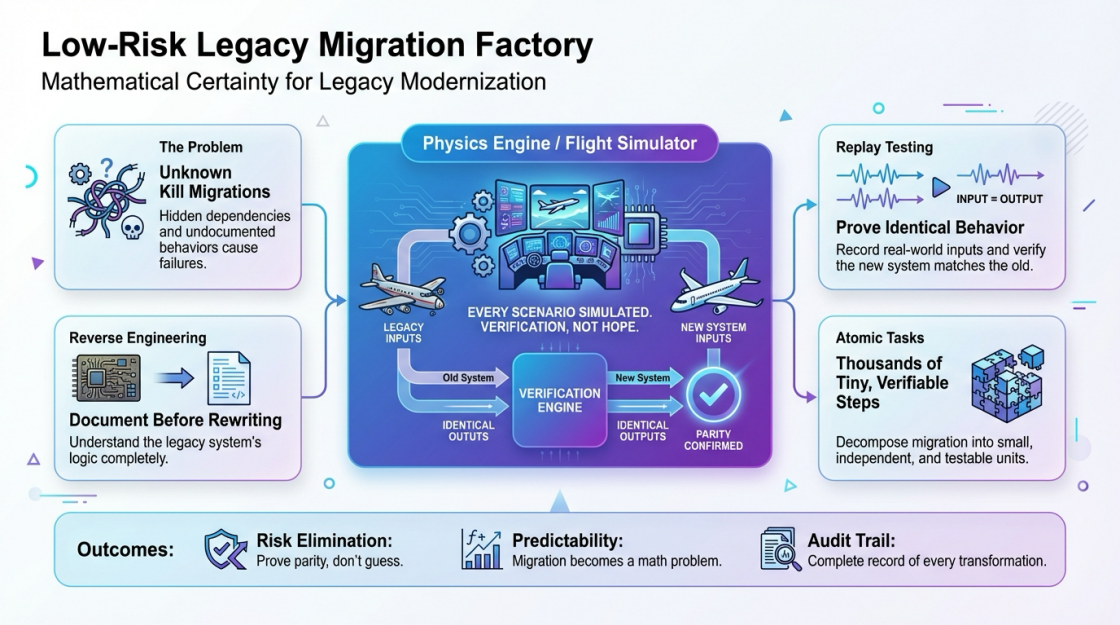


What it is
Production-grade engineering with agents: reliability first via **Test-Driven Agentic Development (TDAD)**, bounded retries, and human gates.

What you get
- TDAD workflow and templates (tests-first patterns) - Self-healing loops with safety stops (no runaway agents) - Human-in-the-loop gates and review practices for high-risk changes

Best for
Teams shipping critical services who want speed without regressions or spaghetti code.

2.3 Low-Risk Legacy Migration Factory

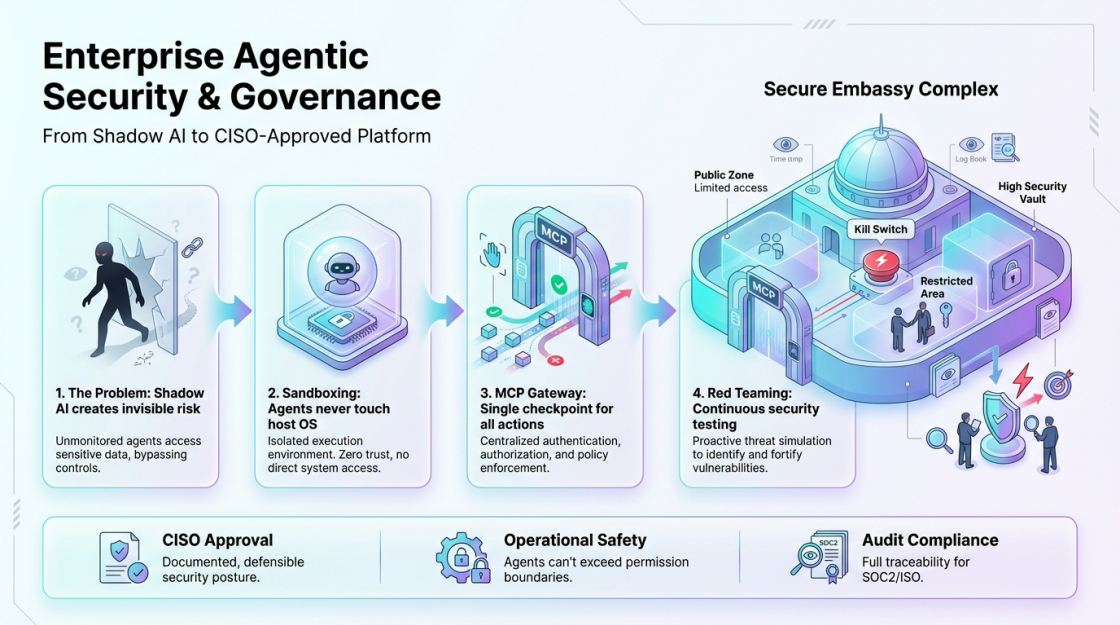


What it is
Modernisation with proof: **verification-by-replay** and simulation patterns that reduce migration risk from “hope” to measurable parity.

What you get
- Replay harness strategy (record → replay → compare outputs) - Atomic task decomposition so changes stay reviewable and testable - A migration playbook that favours evidence over big-bang rewrites

Best for
CTO/CIO-sponsored modernisation where downtime, regressions, and cost overruns are unacceptable.

3.1 Enterprise Agentic Security & Governance

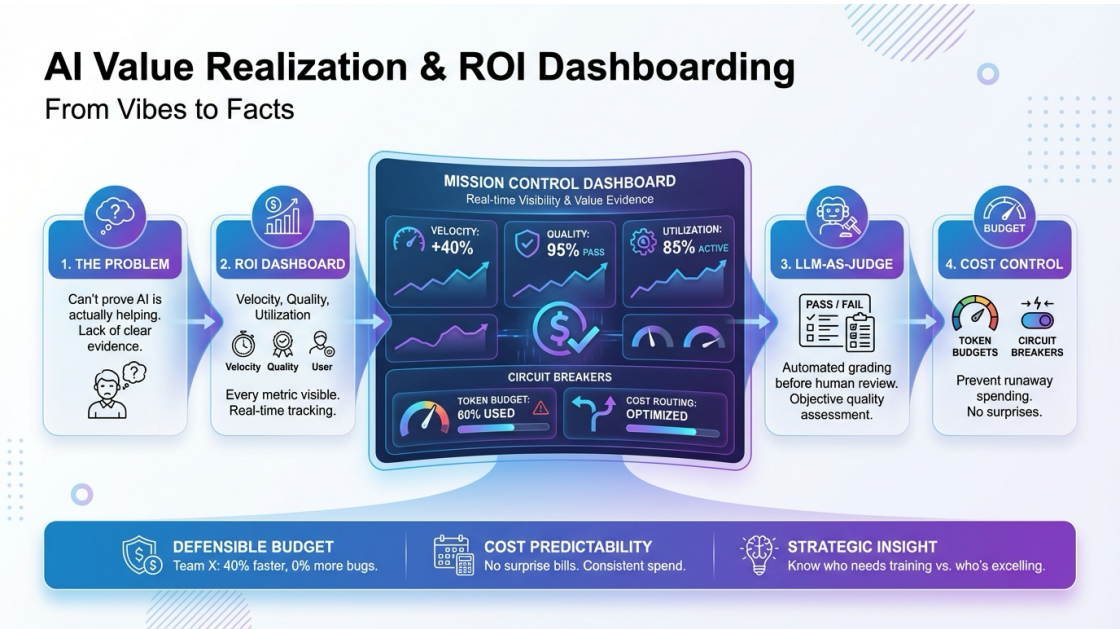


What it is
The security architecture that makes agents deployable: sandboxing, an MCP security gateway, audit logs, and continuous adversarial testing.

What you get
- Secure sandboxing architecture (agents don’t touch the host OS) - MCP gateway model (authn/authz, short-lived tokens, full audit trail) - Permission gating, masking/redaction, and red-team testing approach

Best for
CISOs, security leads, and any organisation blocked by “Shadow AI” risk.

3.2 AI Value Realization & ROI Dashboarding



What it is
A measurement and cost-control system: track utilisation, velocity, quality, and spend; move from “vibes” to defensible ROI.

What you get
- ROI dashboards (utilisation, cycle time, PR throughput, CFR/quality) - LLM-as-a-judge evaluation pipelines (repeatable scoring) - FinOps guardrails (budgets, rate limits, model routing)

Best for
Engineering leadership and finance stakeholders who need proof, predictability, and ongoing improvement.

Commercial Bundles (optional packaging)

Safe Foundation Pack (unlock safe adoption)
- 3.1 Enterprise Agentic Security & Governance
- 1.1 Context Engineering & Knowledge Governance
- 1.3 Enterprise Tooling & Skill Factory

Innovation Pack (prove value fast)
- 2.1 Secure Prototyping Lab
- 2.2 Production Agentic Engineering
- 1.2 Scaling the Agentic Mindset

Big Shift Pack (large-scale transformation)
- 2.3 Low-Risk Legacy Migration Factory
- 3.2 AI Value Realization & ROI Dashboarding

Common engagement shapes

- **2–3 week foundation sprint:** establish baseline controls, first skills, and a rollout plan
- **6–8 week delivery sprint:** prototype → production with measurable outcomes and governance
- **Portfolio / multi-team rollout:** standardise the operating model, tooling, and metrics across orgs

Next step

Share: (1) your top 2–3 use-cases, (2) current constraints from IT/security, and (3) who your champions are. We'll map the fastest safe entry point and the minimum set of offerings to get to production and prove value.