

Benefit

- **AI Enterprise governance and visibility**
- **AI budget control and cost optimisation**
- **Keep sensitive AI traffic within EU/CH data boundaries**
- **Build an effective agentic workforce without exposing IP**

Enterprise AI is becoming infrastructure. Direct model access fragments provider keys, policy enforcement, tool permissions, spend and audit evidence. AI Warden provides an independent control layer across the live AI request path, while cyway operates the platform and integrates it into your security and governance environment.

Approach

Connect: Integrate identity, approved model providers, enterprise DLP, logging and the first business use cases.

Enforce: Inspect prompts, uploads, responses and MCP tool calls. Apply allow, warn, modify, block, budget and containment decisions inline.

Enable: Publish governed chat, model routes, agents and approved tools so users and devs have a practical alternative to shadow AI.

Operate: Secure and reliable onboarding and operations monitors availability and security, maintains the platform, coordinates updates and supports controlled expansion.

Beyond a typical gateway: Combine model routing with enterprise DLP, MCP method controls, agent lifecycle, approvals, budgets and evidence.

Strategic Fit

Establish AI transparency and accountability across business units, suppliers and regulated processes.

Provider independence: Keep Microsoft, AWS, Google investments while applying one policy across them, external and local models.

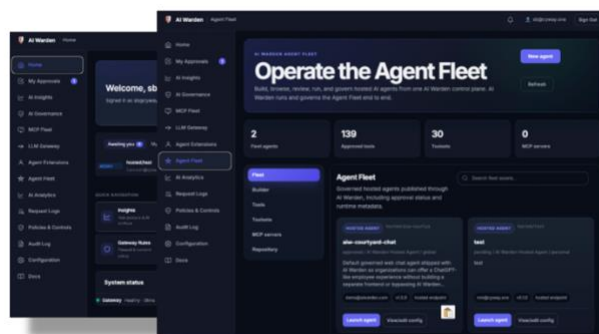
Sovereignty: Deploy the enforcement layer inside approved CH/EU, private or customer-controlled infrastructure.

Regulated operations: Connect identities, DLP decisions, approvals, routes and agent actions into an evidence-ready control trail.

Enable secure innovation while reducing shadow AI, sensitive-data exposure and uncontrolled costs

Deliverables

- **Target architecture and production onboarding** for the AI Warden control plane and gateways
- **Identity, model-provider, DLP and observability integrations** within the agreed scope
- **Approved model aliases, access roles, budgets, routing rules** and initial policy set
- **Governed onboarding workflow** for LLMs, MCP servers, tools and business agents
- **Initial evidence baseline** covering users, agents, policies, DLP outcomes, routes and costs
- **AI Warden platform lifecycle** Coordinated patching, updates and platform maintenance
- **Secure agent enablement** Seamless creation and integration of agents with tailored data, model, tool, policies and context
- **AI Flow Footprint Assessment** (optional) Defensible status baseline of the organization's current AI footprint, distinguish sanctioned from shadow AI



Launch Path

Start with a half-day, on-site Discovery Workshop under NDA. Bring one provider, one MCP server and one DLP policy. Leave with validated integration evidence, a prioritized rollout scope and the decision basis for production.

Put AI into production without losing control.

Request a technical session: cyway.ch/contact