

Nutzen

- **AI Enterprise-Governance und Transparenz**
- **KI-Budgetkontrolle und Kostenoptimierung**
- **Sensiblen KI-Verkehr innerhalb der EU/CH- Grenzen**
- **Leistungsfähige Agenten aufbauen, ohne «IP» offenzulegen**

Enterprise-KI wird zur Infrastruktur. Direkte Modellzugriffe fragmentieren Schlüssel, Richtlinien, Tool-Berechtigungen, Ausgaben und Auditnachweise. AI Warden schafft eine unabhängige Kontrollschicht im produktiven KI-Anfragepfad. cyway betreibt die Plattform und integriert sie in Ihre Sicherheits- und Governance-Umgebung.

Vorgehen

Anbinden: Identitäten, freigegebene Modelle, Enterprise-DLP, Logging und erste Business-Anwendungsfälle integrieren.

Durchsetzen: Prompts, Uploads, Antworten und MCP-Tool-Aufrufe prüfen. Zulassen, Warnen, Ändern, Blockieren, Budgetieren und Eindämmen inline durchsetzen.

Ermöglichen: «Governed Chat», Modellrouten, Agenten und Tools bereitstellen, damit Nutzer und Entwickler eine praxistaugliche Alternative zu Schatten-KI haben.

Betreiben: Sicheres und zuverlässiges Onboarding und Betriebsmanagement überwacht Verfügbarkeit und Sicherheit, wartet die Plattform, koordiniert Updates und den kontrollierten Ausbau.

Mehr als ein typisches Gateway: Modellrouting, Enterprise-DLP, MCP-Kontrollen, Agenten-Lifecycle, Freigaben, Budgets und Nachweise verbinden.

Strategischer Mehrwert

KI-Transparenz und Verantwortlichkeit schaffen in Geschäftsbereichen, bei Lieferanten und in regulierten Prozessen.

Anbieterunabhängigkeit: Microsoft, AWS und Google-Investitionen erhalten; eine Richtlinie auf diese sowie externe und lokale Modelle anwenden.

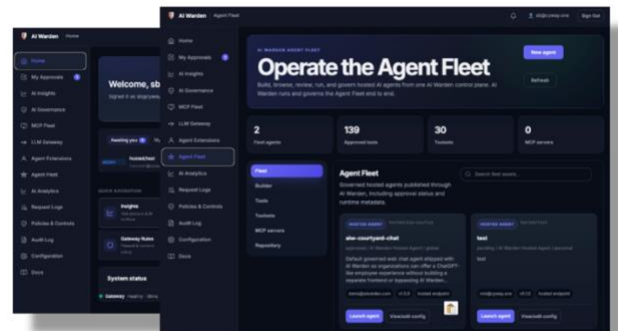
Souveränität: Die Durchsetzungsschicht innerhalb genehmigter CH/EU-, privater oder kundeneigener Infrastruktur betreiben.

Regulierter Betrieb: Identitäten, DLP-Entscheide, Freigaben, Routen und Agentenaktionen revisionsfähig protokollieren.

Sichere Innovation ermöglichen und dabei Schatten-KI, Datenexposition und unkontrollierte Kosten reduzieren

Leistung

- **Zielarchitektur und produktives Onboarding** für die AI-Warden-Kontrollebene und Gateways
- **Integrationen für Identität, Modellanbieter, DLP inkl Audit-Trail**
- **Freigegebene Modelle, Zugriffsrollen, Budgets und Routingregeln** sowie initiales Policy-Set.
- **Governance-konformer Onboarding-Workflow** für LLMs, MCP-Server und Tools sowie Business-Agenten
- **Initiale Nachweisbasis** für Nutzer, Agenten, Richtlinien und DLP-Ergebnisse, Routen und Kosten
- **AI-Warden-Plattform-Lifecycle** Koordinierte Patches, Updates und Plattformwartung
- **Sichere Agentenbefähigung** Nahtlose Erstellung und Integration von Agenten mit zugeschnittenen Daten, Modellen, Tools, Richtlinien und Kontext
- **AI Flow Footprint Assessment** (optional) Belastbare Ist-Aufnahme der aktuellen KI-Landschaft; Unterscheidung zwischen freigegebener und Schatten-KI



Test im Unternehmen

Halbtägiger Discovery Workshop vor Ort unter NDA: ein Anbieter, ein MCP-Server, eine DLP-Richtlinie. Ergebnis: validierte Integration, priorisierter Rollout-Umfang und Entscheidungsgrundlage für die Produktion.

KI produktiv einsetzen, ohne die Kontrolle zu verlieren.

Technische Session anfragen: cyway.ch/contact