



ENTERPRISE AI PLATFORM

Wer hält den Schlüssel zum Königreich

Datensouveränität im Zeitalter von KI

40%

A futuristic robot head with a white, metallic finish and a large, circular, multi-layered eye structure is shown in profile on the left. On the right, a woman with long dark hair, wearing a dark blue shirt, is shown in profile, smiling and looking towards the robot. The background is a bright, clear blue sky.

Digitale Mitarbeiter



Komponenten der Wertschöpfung

Das geistige Eigentum einer Unternehmung

Mitarbeiter

Verfügen über das Fachwissen

Ausbildung, Fachkompetenz und jahrelange Erfahrung stellen das Kapital der Mitarbeiter eines Unternehmens dar. Sie liefern die Impulse und erbringen die geistige und physische Arbeitsleistung

Daten & Prozesse

Erstellen das Produkt

Erstellt, implementiert und gepflegt von Mitarbeitern entstehen so standardisiert und mit hoher Qualität die Produkte und Leistungen eines Unternehmens. Daten und Feedback ermöglichen konstante Optimierung und Wettbewerbsvorteile

Produktivität

Wirtschaftlichkeit

Angetrieben vom institutionellen Wissen der Mitarbeiter und den Prozessen entstehen Marke, Reputation, Produkte und Profite einer Unternehmung.

Das geistige Eigentum und dessen Einsatz erzielen letztendlich unternehmerischen Erfolg.

Dilemma

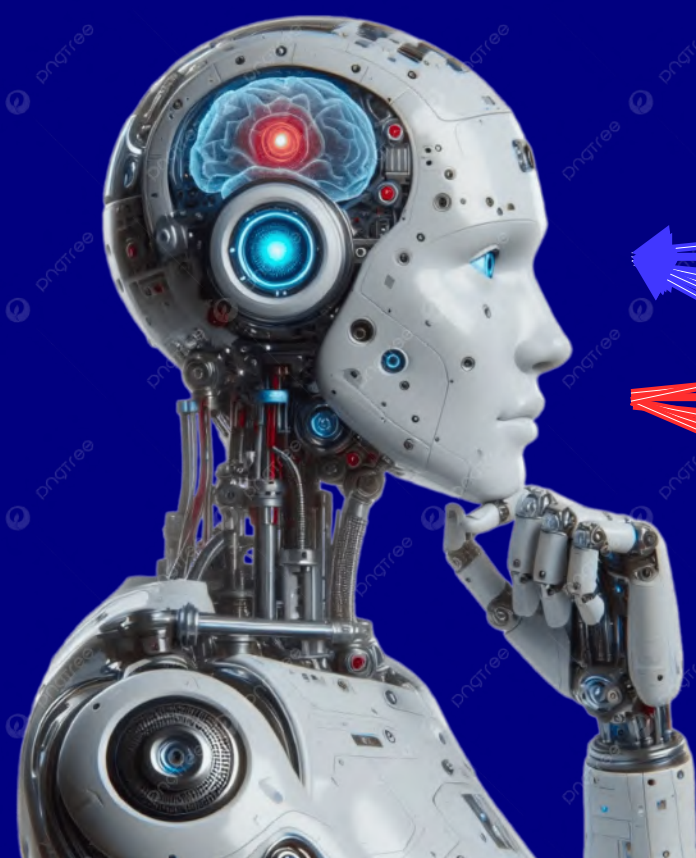






FIREWALL

Unternehmen & Behörden



KI - Anbieter

DATENBANKEN
SOURCECODE
DOKUMENTATION
KUNDENDATEN
FINANZINFORMATIONEN
GEISTIGES EIGENTUM
PRODUKTIONS-SYSTEME



Dilemma





Fundamentale Risiken

Risiken durch KI

Ihre betrieblichen Abläufe sind die Werte des Unternehmens. Sie addieren sich mit der Zeit

Abfluss oder Preisgabe von Know-How

Unachtsamer Einsatz von KI für oft zur Preisgabe von vertraulichen Informationen an unbefugte Personen.

Verlust oder Beschädigung von Daten

Fehlende Kontrollmechanismen erlauben KI und Agenten den vollen Zugriff auf das Unternehmenswissen.

Betriebsunterbrechung

Im Worst Case kann es zu einer Verzögerung oder dem Ausfall der Produktion kommen



Worauf ist zu achten?

Prinzipielle Sicherheitsentscheidungen

Institutionelles Wissen

Daten

Klassifizierung von Daten
und deren Schutzwürdigkeit
Bewusste Entscheidung
zum KI Einsatz
Fallbasierte Freigabe von
Daten und Berechtigungen

Methodenkompetenz

Design

Erstellung von Prozessen
und Pipelines
Multi Agent Kommunikation
Klare Übergabe von Daten
und Ergebnissen

Auditierbarkeit

Kontrolle

Nachvollziehbarkeit von
Prozessen
Speicherung von Audit-
Pfadern
Lernen aus dem Betrieb
(Reinforcement)

Wertschöpfung

Betrieb

Eigene Modelle

Absicherung der
Umgebung
Sandboxed Execution
Open Source

Kosten Kontrolle

KI Forscher und Entwickler erstellen robuste Prozesse im Kontext der Unternehmung mit kontrollierbaren Tools!



Prinzipielle Sicherheits- Entscheidungen

01

Flexibler Betrieb

Im eigenen Rechenzentrum, Cloud VPC, Air-Gapped. Ihre Sicherheitsrichtlinie, Ihre Regeln

02

Granulare Berechtigung

Per-Agent, Per-Team, Per-User Zugriffsrechte. Daten lesen, Schreiben, ausführen.

Analog zum Mitarbeiterzugriff.

03

Protokoll & Audit

Jede Aktion wird protokolliert. Was hat die KI ausgeführt, welche Tools wurden genutzt, welche Entscheidungen sind auf Basis welcher Daten getroffen? Schritt-für-Schritt

04

Isolierte Ausführung

Isolierte Container. Keine Berechtigung in der Umgebung, Netzwerkkontrolle und Schlüssel Management zur Laufzeit

05

Schlüssel-Verwaltung

Zentrale Verwaltung, Verschlüsselung, referenziert über ID's. Keine Hard-Coded Zugriffs-Schlüssel



EIN STRUKTURIERTER ANSATZ IST ERFORDERLICH

Unternehmen mit KI

01

Experten definieren die Ausrichtung

Fachleute beschreiben die Vision und nutzen dazu institutionelles Wissen.

02

Skalierbare Ausführung

Mitarbeiter leiten Agenten an um Ideen in Prozesse mit prüfbaren Resultaten überführen.

03

Optimierung durch Feedback

Deployed solutions and experiments generate unique high-volume, real-world signals.

Punktuelle Lösungen

Wenige profitieren.
Investitionen werden punktuell gestreut. Wenig Synergie

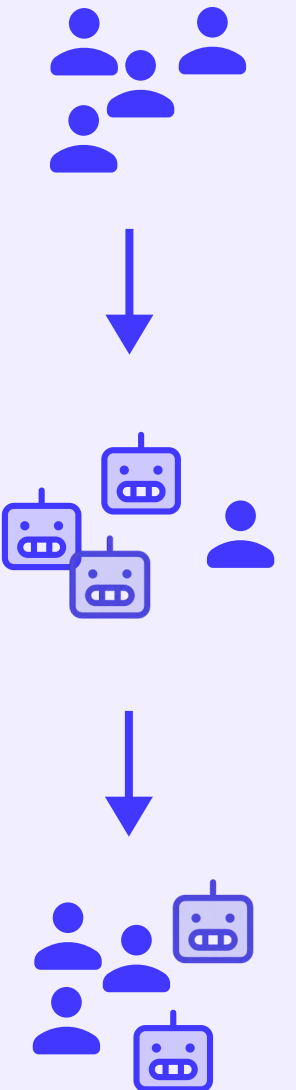


Der Aufbau verursacht die Kosten. Viele Akteure beschäftigen sich mit dem Tun und nicht dem Geschäftserfolg.

Systeme entwickeln sich nicht weiter. Nur wenige Mitarbeiter verbessern und lernen

Zentrale KI Workflows

Viele profitieren.
Investition ermöglicht Differenzierung und Mehrwerte. Kein Implementierungsfokus.



Geringere Einstandskosten,
ermöglichen Experimente und schnellere Innovationszyklen.

Menschen und KI lernen gemeinsam. Optimierte Datennutzung im Prozess.



POOLSIDE & ATOS - PROZESS ENTWICKLUNG

Sicherer Start, Souveränes Wachstum

Beobachtung

KI beobachtet. Menschen entschieden

Abläufen starten parallel zum Team, ergreift aber keine Maßnahmen. Man vergleicht KI Ergebnisse mit den menschlichen Entscheidungen, kalibriert die Parameter. Vertrauen mit echten Daten.

Unterstützung

KI plant. Menschen genehmigen.

Innerhalb der Leitplanken empfiehlt KI Maßnahmen, das Team prüft und genehmigt. Reduktion von Fehlern. Verfeinerung des Setups. Entwickler nutzen in deren Ermessen.

Autonomie

KI führt aus. Menschen behandeln Ausnahmen.

Arbeiten werden von Agenten autark durchgeführt und dabei stets überwacht und bewertet. Menschliche Eingriffe erfolgen nur in Ausnahmefällen. Unternehmensweiter Einsatz

Jeder Betriebsablauf started beobachtend. Menschen entscheiden wann ein Prozess den notwendigen Reifegrad erreicht.

Autonome KI mit Poolside

Wir sind ein Plattformanbieter der eine lokale und autonome Lösung inklusive Modellen, Enterprise Controls liefert und zusammen mit ATOS Prozess Expertise offeriert.

Workflow Automatisierung 

Agenten 

IDE 

CLI 

API 

Foundation Models 

Model Factory 

Trainings Daten (OS Repos + Synthetic) 

=





Q&A



Poolside Informationen

Platform: <https://poolside.ai/blog/introducing-the-poolside-platform>

Modelle: <https://poolside.ai/models>

Unternehmen: <https://poolside.ai/enterprise>

Behörden: <https://poolside.ai/government>

Tech Tools zum Testen:

Pool: <https://poolside.ai/get-started>

Shimmer: <https://shimmer.run/>

Nützliche Links:

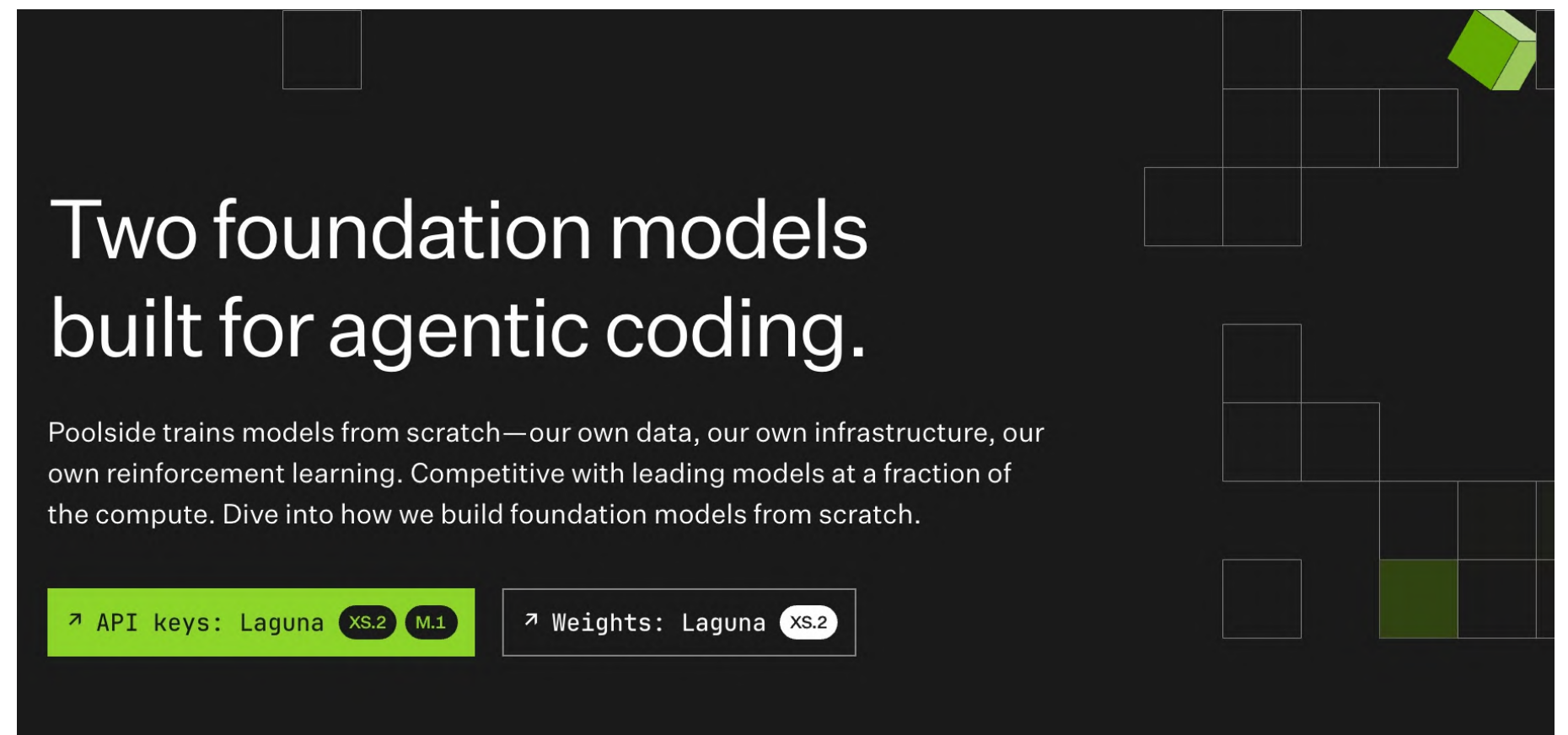
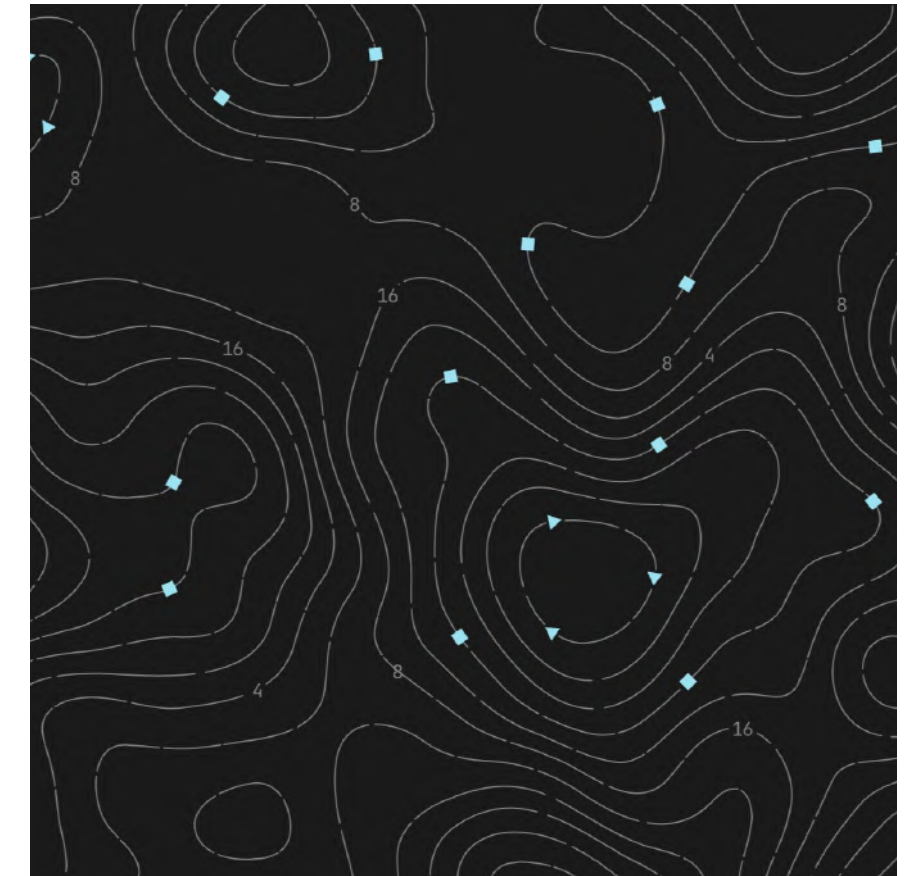
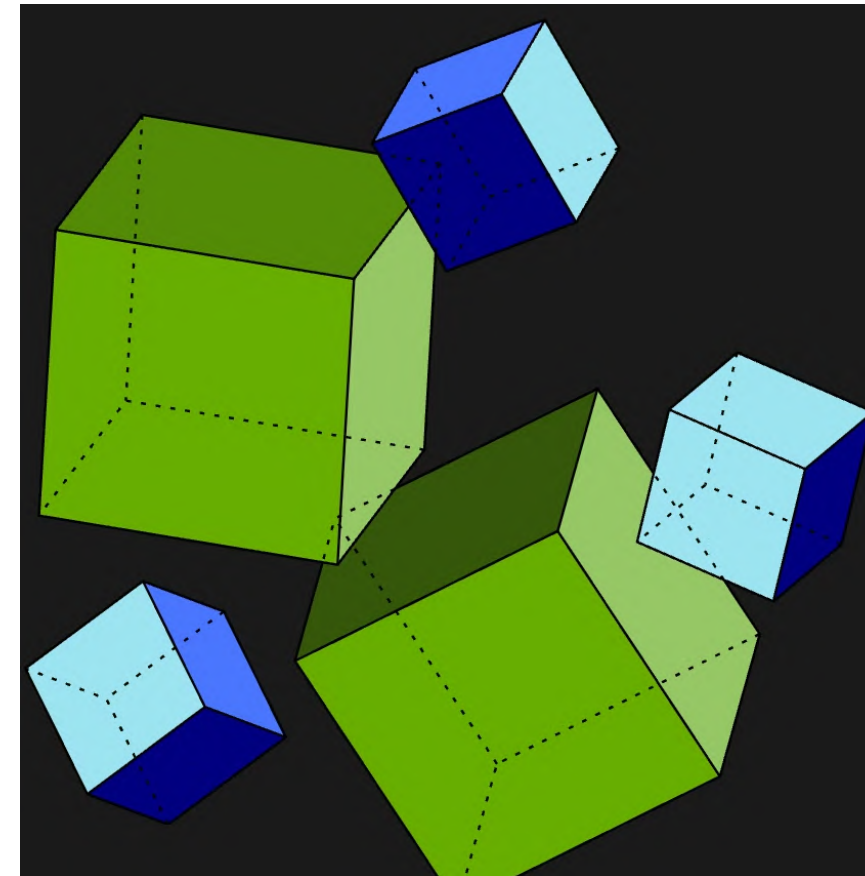
Poolside API: <https://platform.poolside.ai/>

OpenRouter: <https://openrouter.ai/provider/poolside>

Hugging Face: <https://huggingface.co/poolside/Laguna-XS.2>

Ollama: <https://ollama.com/library/laguna-xs.2>

Baseten: <https://www.baseten.co/library/laguna-xs/>



Two foundation models built for agentic coding.

Poolside trains models from scratch—our own data, our own infrastructure, our own reinforcement learning. Competitive with leading models at a fraction of the compute. Dive into how we build foundation models from scratch.

🔗 API keys: Laguna XS.2 M.1

🔗 Weights: Laguna XS.2

Quell: <https://poolside.ai>.