

Kern, Ausstattung, Rahmen

Ich sehe ein Muster: Jeder Anbieter zeigt dir seinen Agenten. Mit drei Ringen kannst du selbst nachsehen, was wirklich drinsteckt.

RL.

Drei Ringe, ein Agent

Die verbindliche Anatomie-Erzählung seit Juli 2026, von innen nach außen gelesen.



01 Kern

Das LLM denkt und entscheidet.

02 Ausstattung

Macht das Modell zum eigenen Agenten.

03 Rahmen

Formt ihn und sichert ihn ab.

Reihenfolge von innen nach außen: der Kern denkt, die Ausstattung handelt, der Rahmen sichert ab.

Kern

Das LLM denkt und entscheidet.

1. **Reasoning** — Mehrschrittig planen, sich selbst korrigieren.
2. **Tool-Calling** — Werkzeuge strukturiert aufrufen.
3. **Instruction-Following** — Sich zuverlässig an Vorgaben halten.
4. **Loop*** — In Schleifen denken. Kommt über die Schnittstelle.

Ausstattung

Macht das Modell zum eigenen Agenten.

1. **Tools** — APIs, Browser, Datenbanken: die Werkzeuge.
2. **Wissen** — Was der Agent nachschlägt.
3. **Skills** — Gebündelte Prozessanweisungen, keine Werkzeuge.
4. **Memory** — Das Gedächtnis selbst, nicht seine Kontrolle.

Rahmen

Formt den Agenten und sichert ihn ab.

1. **Identität** — Persona, Werte, Rolle im Systemprompt.
2. **Guardrails** — Weich im LLM, verbindlich erst technisch.
3. **Prüfstand** — Observability, Tracing, Evals von außen.
4. **Interface** — Format und Ton, die Bühne des Agenten.

Nicht was er hat, sondern was fehlt

Die Frage ist nicht, was ein Agent alles hat. Die Frage ist, welcher Ring leer bleibt.

Starke Ausstattung ohne Rahmen: mächtig und unkontrolliert.
Dicker Rahmen ohne Ausstattung: ein abgesicherter Chatbot.

Altes Wort, neuer Ring

Falls du noch mit Motor, Stimme oder Kompass denkst: hier die Übersetzung, dazu die Regeln in Kurzform und wo das Blatt aufhört.

Instruction-Following ist die Brücke

Instruction-Following im Kern macht den Rahmen erst wirksam.

Ein Modell, das Vorgaben ignoriert, hat weder Identität noch Guardrails. Der äußere Ring greift ins Leere.

Übersetzungstabelle: altes Vokabular im Ringmodell

ALTES WORT	LANDET IM RING	HEISST HEUTE
Motor	Kern	Reasoning, Tool-Calling, Loop
Stimme	Rahmen	Interface
Kompass / Verfassung / Leitplanken	Rahmen	Identität + Guardrails

Die Regeln in Kurzform

1. Ein Agent ist keine Blackbox, sondern drei Ringe: Kern, Ausstattung, Rahmen.
2. Der Loop ist die einzige Kernfähigkeit, die nicht direkt aus dem LLM kommt.
3. Guardrails sind im LLM weich angelegt, verbindlich werden sie erst durch den Rahmen.
4. Instruction-Following macht den Rahmen erst wirksam, sonst greift er ins Leere.
5. Lesen ist harmlos, Schreiben ist das Risiko.

Wofür das Blatt nicht taugt

Das Modell beschreibt Struktur, keine Leistung.
Es sagt nicht, ob ein Agent gut ist, nur woraus er besteht.
Für Marktvergleiche liefert die Quelle keine Zahlen.