

Kann ich kontrollieren, welche KI-Tools mein Unternehmen nutzen darf?

Kurze Antwort: Ja. FortressAI bietet eine Bewertung pro Tool — granulare Kontrolle darüber, welche KI-Tools genau autorisiert und welche blockiert sind — sowie standortbasierte Durchsetzung, sodass Richtlinien an den Ort geknüpft werden können, an dem sensible Daten liegen, statt an einzelne Anwendungen.

Zwei sich ergänzende Kontrollmechanismen

- **Bewertung pro Tool:** Legen Sie gezielt fest, welche KI-Anwendungen (Gemini, Copilot und andere) in Ihrer Umgebung zulässig sind.
- **Standortbasierte Durchsetzung:** Definieren Sie Schutzmaßnahmen rund um die relevanten Datenstandorte — sodass Quellcode im Repository verbleibt und nicht in einem Chatbot landet — wobei die Zuweisungen von den Nutzern gesteuert werden.

Das Ampelprinzip (Traffic Light Protocol)

Die FortressAI-Richtlinie wird als Ampel dargestellt:

- **Rot** — FortressAI blockiert den Zugriff des KI-Tools auf die zugewiesenen Daten.
- **Gelb** — der Zugriff wird bedingt bewertet, einschließlich dynamischer Behandlung sensibler Daten. *(Die bedingten Abläufe, die von der Purview/MIP-Label-Durchsetzung und der automatischen PII/PDPL-Anonymisierung abhängen, befinden sich in der Beta-Phase — siehe „Welche FortressAI-Funktionen sind allgemein verfügbar und welche befinden sich in der Beta-Phase?“)*
- **Grün** — die genehmigte Nutzung erfolgt normal.

Dies ermöglicht es Unternehmen, KI bewusst einzuführen, anstatt zwischen pauschalen Verboten, die umgangen werden, und einem offenen Zugang, der Daten preisgibt, wählen zu müssen.

Revision #1

Created 2026-07-24 04:36:55 UTC by Dennis Underwood

Updated 2026-07-24 04:36:55 UTC by Dennis Underwood