Can I control which AI tools my organization is allowed to use?

Short answer: Yes. FortressAI provides per-tool assessment — granular control over exactly which AI tools are authorized and which are blocked — and location-based enforcement, so policy can be tied to where sensitive data lives rather than to individual applications.

Two complementary controls

- **Per-tool assessment:** decide specifically which AI applications (Gemini, Copilot, and others) are permitted in your environment.
- **Location-based enforcement:** define protection around the data locations that matter — keeping source code in the repository, not in a chatbot — with assignments controlled by users.

The Traffic Light Protocol

FortressAI policy is expressed as a traffic light:

- **Red** — FortressAI blocks the AI tool from accessing the assigned data.
- **Yellow** — access is evaluated conditionally, including dynamic handling of sensitive data. *(The conditional paths that depend on Purview/MIP label enforcement and automatic PII/PDPL anonymization are in beta — see "Which FortressAI capabilities are generally available, and which are in beta?")*
- **Green** — approved use proceeds normally.

This lets organizations adopt AI deliberately rather than choosing between blanket bans that get worked around and open access that leaks data.

Revision #3
Created 2026-07-20 19:24:01 UTC by Dennis Underwood
Updated 2026-07-21 19:32:16 UTC by Dennis Underwood