Shadow AI: Block First, Then Govern

Surveys regularly find that many employees use AI tools their employer hasn't approved. Framed as "the problem", that points teams in the wrong direction. The problem isn't that people reach for useful tools — it's that most organizations have no way to see or control what those tools touch. The practical path is to gain control first, then layer governance on top.

Start by regaining control

When security leaders first open a control plane like the FortressAI portal, the deep, granular options are available — but that's rarely where they begin. Most start exhausted by the topic and want one thing: to block access and establish control. "I don't want ChatGPT reaching the network shares. I don't want this tool executing at all." Blocking unsanctioned AI execution at the kernel layer is a clean, decisive first step that stops the bleeding without requiring a finished policy.

Then move from "block all" to "allow by intent"

Control is the foundation for nuance. Once everything is blocked except a known-good baseline, teams start writing the rules they actually want:

- Developers may use an AI assistant **on the developer server**.
- That same assistant must **never** touch the **payroll server**.
- Specific tools are approved for specific groups and specific data.

This intent-based model only becomes possible *after* you can enforce it. You can't write "developers only, never payroll" if you can't see or stop AI activity per system in the first place.

Why order matters

Trying to author perfect AI policy before you have enforcement is how shadow AI persists — the policy exists on paper while unsanctioned tools keep running. Blocking first gives you a known state to build from; governance then expands the allowed surface deliberately, tool by tool and system by system.

The takeaway: shadow AI is a control gap, not a headcount problem. Establish kernel-level control over what AI can execute and reach, then open access on your terms.

Adapted from a conversation with Cyber Crucible founder Dennis Underwood.

Revision #1
Created 2026-11-24 04:48:57 UTC by Dennis Underwood
Updated 2026-11-24 04:48:57 UTC by Dennis Underwood