

What is FortressAI?

Short answer: FortressAI is Cyber Crucible's generative-AI data protection product. It enforces policy at the operating system's deepest layer, checking data access on the device and blocking, redacting, or safely allowing information before it can reach ChatGPT, Copilot, Gemini, or any other AI tool.

The problem it solves

Public AI tools are transforming how people work, and simultaneously opening a new path for data to leave an organization. Every prompt carries risk. Employees frequently share sensitive information without realizing they've done anything wrong, and traditional security tools were never designed for this.

Why kernel-level enforcement matters here

FortressAI operates at the same depth as the rest of the Cyber Crucible platform. That means it protects against *any* AI tool — including ones that don't exist yet — rather than maintaining a list of specific applications to police. It doesn't need to understand a new AI product to stop sensitive data from reaching it.

Because enforcement is local, prompt content is never shipped to a cloud service for inspection. The protection doesn't create the exposure it's meant to prevent.

FortressAI is not a separate engine bolted on. It is a policy layer over the same kernel memory behavioral analytics that drive data and identity protection — which is how it can judge not just whether an AI tool is approved, but whether it has been tampered with.

Revision #3

Created 2026-07-20 19:23:56 UTC by Dennis Underwood

Updated 2026-07-21 19:32:12 UTC by Dennis Underwood