How does FortressAI help with compliance and audit?

Short answer: FortressAI prevents the leak rather than reporting it afterward, and provides straightforward records of who accessed what and where leaks were stopped — evidence you can show an auditor.

Prevention as a compliance posture

Most compliance exposure from AI use follows the same pattern: sensitive data leaves the organization, and the obligation to investigate, notify, or disclose follows. Blocking the access at the kernel means the disclosure event doesn't occur.

Demonstrating control

Auditors and regulators generally want two things: evidence that a control exists, and evidence that it works. FortressAI supports both — a policy that is technically enforced at the operating system level, and clear records showing where enforcement occurred.

Where this applies

The requirement shows up under many frameworks — HIPAA for patient information, FERPA for student records, GDPR for personal data, and contractual confidentiality obligations. The underlying control is the same in each case: sensitive data must not leave the boundary, and you must be able to prove it didn't.

Revision #3
Created 2026-07-20 19:24:03 UTC by Dennis Underwood
Updated 2026-07-21 19:32:18 UTC by Dennis Underwood