Wie unterstützt FortressAI bei Compliance und Audits?

Kurze Antwort: FortressAI verhindert das Datenleck, anstatt es im Nachhinein zu melden, und liefert klare Aufzeichnungen darüber, wer worauf zugegriffen hat und wo Lecks gestoppt wurden — Nachweise, die Sie einem Auditor vorlegen können.

Prävention als Compliance-Haltung

Die meisten Compliance-Risiken bei der Nutzung von KI folgen demselben Muster: Sensible Daten verlassen die Organisation, und daraus ergibt sich die Verpflichtung zur Untersuchung, Benachrichtigung oder Offenlegung. Wird der Zugriff bereits auf Kernel-Ebene blockiert, tritt das Offenlegungsereignis gar nicht erst ein.

Kontrolle nachweisen

Auditoren und Regulierungsbehörden erwarten in der Regel zweierlei: den Nachweis, dass eine Kontrolle existiert, und den Nachweis, dass sie funktioniert. FortressAI unterstützt beides — eine Richtlinie, die technisch auf Betriebssystemebene durchgesetzt wird, sowie klare Aufzeichnungen, die zeigen, wo die Durchsetzung erfolgt ist.

Wo dies zur Anwendung kommt

Diese Anforderung findet sich in vielen Rahmenwerken wieder — HIPAA für Patientendaten, FERPA für Schülerdaten, GDPR für personenbezogene Daten sowie vertragliche Vertraulichkeitspflichten. Die zugrunde liegende Kontrolle ist in jedem Fall dieselbe: Sensible Daten dürfen die Grenze nicht verlassen, und Sie müssen nachweisen können, dass dies auch nicht geschehen ist.

Revision #1
Created 2026-07-24 04:37:16 UTC by Dennis Underwood
Updated 2026-07-24 04:37:16 UTC by Dennis Underwood