

Was ist FortressAI?

Kurze Antwort: FortressAI ist das generative-KI-Datenschutzprodukt von Cyber Crucible. Es setzt Richtlinien auf der tiefsten Ebene des Betriebssystems durch, überprüft den Datenzugriff auf dem Gerät und blockiert, redigiert oder erlaubt Informationen sicher, bevor sie ChatGPT, Copilot, Gemini oder ein anderes KI-Tool erreichen können.

Das Problem, das es löst

Öffentliche KI-Tools verändern die Art und Weise, wie Menschen arbeiten, und eröffnen gleichzeitig einen neuen Weg, auf dem Daten ein Unternehmen verlassen können. Jeder Prompt birgt ein Risiko. Mitarbeiter teilen häufig sensible Informationen, ohne zu bemerken, dass sie etwas falsch gemacht haben, und herkömmliche Sicherheitstools wurden nie für diesen Zweck entwickelt.

Warum die Durchsetzung auf Kernel-Ebene hier von Bedeutung ist

FortressAI arbeitet auf derselben Tiefe wie der Rest der Cyber-Crucible-Plattform. Das bedeutet, dass es vor *jedem* KI-Tool schützt – einschließlich solcher, die noch gar nicht existieren – anstatt eine Liste bestimmter Anwendungen zu pflegen, die überwacht werden müssen. Es muss ein neues KI-Produkt nicht verstehen, um zu verhindern, dass sensible Daten dorthin gelangen.

Da die Durchsetzung lokal erfolgt, wird der Prompt-Inhalt niemals zur Überprüfung an einen Cloud-Dienst übermittelt. Der Schutz schafft nicht die Gefährdung, die er eigentlich verhindern soll.

FortressAI ist keine separat angebaute Engine. Es ist eine Richtlinienenebene über derselben verhaltensbasierten Kernel-Speicheranalyse, die auch den Daten- und Identitätsschutz antreibt – und genau dadurch kann es nicht nur beurteilen, ob ein KI-Tool zugelassen ist, sondern auch, ob es manipuliert wurde.

Revision #1

Created 2026-07-24 04:36:02 UTC by Dennis Underwood

Updated 2026-07-24 04:36:03 UTC by Dennis Underwood