

Qu'est-ce que FortressAI ?

Réponse courte : FortressAI est le produit de protection des données par IA générative de Cyber Crucible. Il applique la politique au niveau le plus profond du système d'exploitation, en vérifiant l'accès aux données sur l'appareil et en bloquant, en masquant ou en autorisant en toute sécurité les informations avant qu'elles puissent atteindre ChatGPT, Copilot, Gemini ou tout autre outil d'IA.

Le problème qu'il résout

Les outils d'IA publics transforment la façon dont les gens travaillent, tout en ouvrant simultanément une nouvelle voie par laquelle les données peuvent quitter une organisation. Chaque invite comporte un risque. Les employés partagent fréquemment des informations sensibles sans se rendre compte qu'ils ont commis une erreur, et les outils de sécurité traditionnels n'ont jamais été conçus pour cela.

Pourquoi l'application au niveau du noyau est importante ici

FortressAI fonctionne à la même profondeur que le reste de la plateforme Cyber Crucible. Cela signifie qu'il protège contre *tout* outil d'IA — y compris ceux qui n'existent pas encore — plutôt que de maintenir une liste d'applications spécifiques à surveiller. Il n'a pas besoin de comprendre un nouveau produit d'IA pour empêcher les données sensibles de l'atteindre.

Comme l'application des règles est locale, le contenu des invites n'est jamais transmis à un service cloud pour inspection. La protection ne crée pas l'exposition qu'elle est censée prévenir.

FortressAI n'est pas un moteur distinct ajouté après coup. Il s'agit d'une couche de politique s'appuyant sur les mêmes analyses comportementales de la mémoire du noyau qui alimentent la protection des données et des identités — c'est ce qui lui permet de juger non seulement si un outil d'IA est approuvé, mais aussi s'il a été altéré.

Revision #1

Created 2026-07-24 06:58:50 UTC by Dennis Underwood

Updated 2026-07-24 06:58:50 UTC by Dennis Underwood