

# ¿Qué es FortressAI?

**Respuesta breve:** FortressAI es el producto de protección de datos de IA generativa de Cyber Crucible. Aplica la política en la capa más profunda del sistema operativo, verificando el acceso a los datos en el dispositivo y bloqueando, redactando o permitiendo de forma segura la información antes de que pueda llegar a ChatGPT, Copilot, Gemini o cualquier otra herramienta de IA.

## El problema que resuelve

Las herramientas públicas de IA están transformando la forma en que las personas trabajan, y al mismo tiempo abren una nueva vía para que los datos salgan de una organización. Cada indicación (prompt) conlleva un riesgo. Los empleados con frecuencia comparten información sensible sin darse cuenta de que han hecho algo incorrecto, y las herramientas de seguridad tradicionales nunca fueron diseñadas para esto.

## Por qué la aplicación a nivel de kernel es importante aquí

FortressAI opera a la misma profundidad que el resto de la plataforma Cyber Crucible. Esto significa que protege contra *cualquier* herramienta de IA — incluidas aquellas que aún no existen — en lugar de mantener una lista de aplicaciones específicas para vigilar. No necesita entender un nuevo producto de IA para impedir que los datos sensibles lleguen a él.

Debido a que la aplicación es local, el contenido de las indicaciones nunca se envía a un servicio en la nube para su inspección. La protección no crea la exposición que pretende prevenir.

FortressAI no es un motor separado añadido posteriormente. Es una capa de política sobre el mismo análisis conductual de la memoria del kernel que impulsa la protección de datos e identidad, lo cual es lo que le permite evaluar no solo si una herramienta de IA está aprobada, sino también si ha sido manipulada.

---

Revision #1

Created 2026-07-24 01:49:51 UTC by Dennis Underwood

Updated 2026-07-24 01:49:51 UTC by Dennis Underwood