¿Cómo protege FortressAI los datos en un navegador web?

> **Capacidad en beta.** La detección y aplicación de políticas de uso de IA basada en navegador se encuentra actualmente en fase beta. Es funcional y está en uso activo, pero evalúela en su entorno antes de depender de ella como control.

Respuesta breve: FortressAI supervisa la actividad del navegador desde el kernel y la evalúa conforme a la política. Si el navegador, un sitio web o una extensión intenta acceder a datos fuera de la política, el permiso se revoca en la capa del kernel; y si el navegador muestra señales de explotación, se revocan todos los derechos de acceso a los datos y se suspende el proceso.

La secuencia

1. Un usuario abre un navegador web — Edge, Chrome o Firefox.
2. La supervisión a nivel de kernel evalúa el navegador y cualquier actividad de página o extensión conforme a la política de FortressAI asignada.
3. Si el navegador, el sitio o la extensión intenta acceder a datos fuera de la política, el permiso se revoca en la capa del kernel.
4. Si el navegador muestra señales de explotación, se revocan todos los derechos de acceso a los datos y se suspende el proceso.

Por qué el navegador es el punto de control crítico

El navegador es donde realmente ocurre la mayor parte del uso de IA generativa, y también es una superficie de ataque intensamente atacada. Cyber Crucible lo ha comprobado de manera directa: desde el cuarto trimestre de 2023 en adelante, las respuestas automatizadas contra la actividad de Chrome, Edge y Chromium pasaron de cero a miles, con los CVE relacionados publicados posteriormente por Google y Microsoft. En una empresa, el patrón escaló de un puñado de ataques bloqueados a casi 4,000 en prácticamente todas las estaciones de trabajo.

Revision #1
Created 2026-07-24 01:50:16 UTC by Dennis Underwood
Updated 2026-07-24 01:50:16 UTC by Dennis Underwood