Como o FortressAI protege dados em um navegador web?

> **Capacidade em beta.** A detecção e aplicação de políticas de uso de IA baseada em navegador está atualmente em beta. Ela é funcional e está em uso ativo, mas avalie-a em seu ambiente antes de depender dela como um controle.

Resposta curta: O FortressAI monitora a atividade do navegador a partir do kernel e a avalia em relação à política. Se o navegador, um site ou uma extensão tentar acessar dados fora da política, a permissão é revogada na camada do kernel — e, se o navegador apresentar sinais de exploração, todos os direitos de acesso a dados são revogados e o processo é suspenso.

A sequência

1. Um usuário abre um navegador web — Edge, Chrome ou Firefox.
2. O monitoramento em nível de kernel avalia o navegador e qualquer atividade de página ou extensão em relação à política do FortressAI atribuída.
3. Se o navegador, o site ou a extensão tentar acessar dados fora da política, a permissão é revogada na camada do kernel.
4. Se o navegador apresentar sinais de exploração, todos os direitos de acesso a dados são revogados e o processo é suspenso.

Por que o navegador é o ponto de controle crítico

O navegador é onde a maior parte do uso de IA generativa realmente acontece, e também é uma superfície de ataque fortemente visada. A Cyber Crucible tem observado isso diretamente: a partir do quarto trimestre de 2023, as respostas automatizadas contra atividades do Chrome, Edge e Chromium aumentaram de zero para milhares, com CVEs relacionados posteriormente publicados pelo Google e pela Microsoft. Em uma empresa, o padrão escalou de um punhado de ataques bloqueados para quase 4.000 em praticamente todas as estações de trabalho.

Revision #1
Created 2026-07-24 05:48:35 UTC by Dennis Underwood
Updated 2026-07-24 05:48:35 UTC by Dennis Underwood