Wie schützt FortressAI Daten in einem Webbrowser?

> **Beta-Funktion.** Die browserbasierte Erkennung und Durchsetzung der KI-Nutzung befindet sich derzeit in der Beta-Phase. Sie ist funktionsfähig und im aktiven Einsatz, sollte jedoch in Ihrer Umgebung evaluiert werden, bevor Sie sich darauf als Kontrollmechanismus verlassen.

Kurze Antwort: FortressAI überwacht die Browseraktivität auf Kernel-Ebene und bewertet sie anhand der Richtlinie. Wenn der Browser, eine Website oder eine Erweiterung versucht, außerhalb der Richtlinie auf Daten zuzugreifen, wird die Berechtigung auf Kernel-Ebene entzogen — und wenn der Browser Anzeichen einer Ausnutzung (Exploitation) zeigt, werden sämtliche Datenrechte entzogen und der Prozess wird angehalten.

Der Ablauf

1. Ein Benutzer öffnet einen Webbrowser — Edge, Chrome oder Firefox.
2. Die Überwachung auf Kernel-Ebene bewertet den Browser sowie jegliche Seiten- oder Erweiterungsaktivität anhand der zugewiesenen FortressAI-Richtlinie.
3. Wenn der Browser, die Website oder die Erweiterung versucht, außerhalb der Richtlinie auf Daten zuzugreifen, wird die Berechtigung auf Kernel-Ebene entzogen.
4. Wenn der Browser Anzeichen einer Ausnutzung zeigt, werden sämtliche Datenrechte entzogen und der Prozess wird angehalten.

Warum der Browser der entscheidende Kontrollpunkt ist

Der Browser ist der Ort, an dem der Großteil der generativen KI-Nutzung tatsächlich stattfindet, und er ist zugleich eine stark angegriffene Angriffsfläche. Cyber Crucible hat dies unmittelbar beobachtet: Seit dem vierten Quartal 2023 sind automatisierte Reaktionen auf Aktivitäten von Chrome, Edge und Chromium von null auf mehrere Tausend gestiegen, wobei anschließend entsprechende CVEs von Google und Microsoft veröffentlicht wurden. Bei einem Unternehmen eskalierte das Muster von einer Handvoll blockierter Angriffe auf nahezu 4.000 über nahezu jede Workstation hinweg.

Revision #1
Created 2026-07-24 04:36:31 UTC by Dennis Underwood
Updated 2026-07-24 04:36:31 UTC by Dennis Underwood