Comment Cyber Crucible facilite-t-il la conformité FERPA et la protection des données des étudiants ?

Réponse courte : FortressAI vérifie l'accès aux données directement sur l'appareil, afin que les dossiers des étudiants et les données familiales ne puissent pas atteindre accidentellement un outil d'IA public. Cyber Crucible stoppe les rançongiciels de manière autonome, sans nécessiter de centre opérationnel de sécurité (SOC) disponible 24 h/24 et 7 j/7 — une contrainte que la plupart des établissements scolaires ne peuvent pas financer.

Les deux problématiques du secteur éducatif

Les écoles et universités sont des cibles privilégiées des rançongiciels, tout en disposant rarement du budget nécessaire pour assurer une surveillance permanente. Dans le même temps, l'adoption de l'IA en classe a progressé bien plus vite que sa gouvernance.

Répondre aux deux enjeux

- **Rançongiciels sans SOC :** une prévention autonome, au niveau du noyau, stoppe les attaques en moins de 200 millisecondes, sans qu'il soit nécessaire d'embaucher des analystes ni de financer un contrat de surveillance 24 h/24 et 7 j/7.
- **Usage de l'IA conforme à la FERPA :** FortressAI évalue chaque requête directement sur l'appareil, afin que les dossiers scolaires protégés et les données personnelles des familles ne se retrouvent pas dans un système d'IA public — y compris en tant que données d'entraînement.

Cette combinaison protège les étudiants et le personnel sans ajouter de charge informatique significative.

Revision #1
Created 2026-07-24 07:00:38 UTC by Dennis Underwood
Updated 2026-07-24 07:00:38 UTC by Dennis Underwood