# Como apoia a Cyber Crucible a privacidade dos dados dos estudantes em escolas e universidades?

**Resposta breve:** A Cyber Crucible ajuda instituições de ensino de duas formas: interrompe o ransomware de forma autónoma sem necessidade de um centro de operações de segurança (SOC) 24/7, e — através da FortressAI — avalia o acesso a dados por ferramentas de IA no dispositivo, para que os registos dos estudantes e os dados familiares não cheguem acidentalmente a um sistema de IA público. Como a análise é local e não são recolhidos registos de estudantes, os registos educativos protegidos permanecem dentro do perímetro da instituição.

**Saiba mais:** proteção contra ransomware para escolas e universidades

# Os dois problemas educativos abordados

- **Ransomware sem um SOC.** A prevenção ao nível do kernel interrompe os ataques em menos de 200 milissegundos, sem necessidade de contratar analistas nem de financiar um contrato de monitorização contínua 24/7.
- **Governação de IA para a sala de aula.** A FortressAI impede que os registos educativos protegidos e os dados pessoais familiares cheguem a ferramentas de IA e a LLM, mediante políticas aplicadas no próprio dispositivo, para que não sejam enviados para um sistema de IA público — nem sequer como dados de treino.

# Notas para a seleção de fornecedores

- A Cyber Crucible atua sob a direção da instituição e não utiliza os dados dos estudantes para qualquer finalidade secundária.
- As leis estaduais de privacidade de estudantes (por exemplo, na Califórnia, em Nova Iorque e no Colorado) acrescentam obrigações adicionais aos fornecedores; o design de processamento local e sem recolha de dados dá suporte a essas exigências. A documentação está disponível mediante acordo de confidencialidade (NDA).

Revision #3
Created 2026-07-24 06:02:59 UTC by Dennis Underwood
Updated 2026-11-24 15:49:37 UTC by Dennis Underwood