What compliance risk does encryption key escrow create, and why doesn't Cyber Crucible do it?

Short answer: Storing encryption keys centrally creates a single point of failure, a high-value target, and exposure to compelled disclosure. Cyber Crucible's prevention approach doesn't depend on capturing or escrowing keys, so there is no central key store to secure, subpoena, or breach.

> For the direct product answer, see the existing article **"Does Cyber Crucible collect encryption keys?"** This page covers the compliance and data-sovereignty reasoning behind that answer.

Why this is deliberate

Cyber Crucible originally developed and patented key-capture technology for ransomware defense. By 2021, ransomware strains had evolved to defeat it — using custom encryption libraries, unique per-execution implementations, and streaming ciphers immune to key capture. We presented that cryptanalysis publicly at BSides Pittsburgh in 2021.

The risk we chose not to create

Beyond no longer working, key capture requires centralized storage of encryption keys. That introduces a single point of failure, a high-value target, and the possibility of compelled disclosure without customer knowledge.

Preventing the attack before encryption begins removes the need for keys entirely — which is both a stronger defense and a smaller compliance surface.

Revision #3
Created 2026-07-20 19:24:08 UTC by Dennis Underwood
Updated 2026-07-21 19:32:23 UTC by Dennis Underwood