How does Cyber Crucible support HIPAA compliance in healthcare?

Short answer: All analysis happens locally at the kernel level, so protected health information never leaves the endpoint for security processing. That avoids the HIPAA exposure created by security tools that upload sensitive files or keys to third-party clouds, and it stops attacks without taking clinical systems offline.

The problem with vendor-hosted security

Many vendor-hosted SOC and MDR arrangements require uploading sensitive keys, files, or telemetry to third-party cloud databases. For a covered entity, that creates real compliance risk and expands the number of parties handling protected data.

Local analysis, local data

Cyber Crucible analyzes on the endpoint. Sensitive assets never leave the secure boundary of the device — which supports both data sovereignty and the regulatory position that goes with it.

Continuity matters clinically

Containment that requires isolating a machine or forcing a reboot is not acceptable when patient care depends on it. Selective suspension of only the malicious process means the attack is neutralized in under 200 milliseconds while medical operations, connected devices, and clinical systems keep running.

Revision #3
Created 2026-07-20 19:24:05 UTC by Dennis Underwood
Updated 2026-07-21 19:32:20 UTC by Dennis Underwood