How does Cyber Crucible protect law firms and professional-services confidentiality?

Short answer: Cyber Crucible protects privileged and confidential client material by keeping analysis on the endpoint and never collecting files, credentials, or keys — so client confidences are not exposed to a third-party cloud in the course of being protected. It stops ransomware and infostealers autonomously, which matters for firms without a large security team.

Why it fits professional services

- **Confidentiality by design.** No client documents leave the device for security processing; there is no vendor-held copy to subpoena or breach.
- **Identity and data theft prevention.** Infostealers targeting session tokens and credentials are intercepted before data leaves the device.
- **Low operational overhead.** Autonomous prevention works without a 24/7 SOC.

Vendor-selection notes

Ethical duties of confidentiality and, for many firms, client security addenda drive vendor scrutiny; the no-collection, local-processing model supports both. A data processing agreement is available on request.

Revision #2
Created 2026-07-23 15:18:30 UTC by Dennis Underwood
Updated 2026-07-23 18:20:00 UTC by Dennis Underwood