How does Cyber Crucible support CMMC and DFARS requirements for the defense industrial base?

Short answer: Cyber Crucible is not CMMC-certified, and it says so plainly. It supports a defense contractor's obligations under DFARS 252.204-7012 and CMMC primarily by not collecting Controlled Unclassified Information (CUI) and by supporting on-premises or air-gapped deployment inside the contractor's own boundary, where CUI stays under the contractor's control.

Learn more: air-gapped ransomware protection for the defense industrial base

How it supports the contractor's obligations

- **No CUI collected.** The endpoint agent analyzes behavior locally without extracting the files it protects, so CUI is not transferred to Cyber Crucible.
- **Boundary-preserving deployment.** On-premises and air-gapped models keep all data within the contractor's assessed boundary.
- **Endpoint protection controls.** Malware/ransomware prevention and monitoring map to the relevant CMMC practices and NIST SP 800-171 controls the contractor must implement.
- **US supply chain.** US data is handled by US-based resources; offshore contractors do not handle US data or develop the agents. The software is EAR-controlled, not ITAR.

The honest boundary

CMMC certification is held by the contractor's environment, not by an individual security tool; Cyber Crucible is a control that supports several 800-171 requirements, not a substitute for the contractor's assessment. Mapping detail is available under NDA.

Revision #4
Created 2026-07-23 15:18:24 UTC by Dennis Underwood
Updated 2026-11-24 15:45:21 UTC by Dennis Underwood