How does Cyber Crucible protect manufacturing, OT, and ICS environments?

Short answer: It runs entirely on the endpoint with no cloud dependency, so it protects operational technology and industrial control systems that are offline, air-gapped, or intermittently connected — and it suspends only the malicious process, so production keeps moving.

Why conventional tools struggle here

OT and ICS environments can tolerate neither a cloud round trip nor a full-network lockdown. Many are deliberately disconnected. Security models that assume constant connectivity and a remote SOC simply don't apply.

What changes

- **100% offline capable** — full protection with no signal required, air-gap ready.
- **No lockdowns** — malicious processes are suspended in memory while production continues.
- **One agent across the environment** — the same lightweight agent protects PLCs on the plant floor, vehicles across a logistics network, and vessels at sea, with no analyst in the loop and no connectivity assumptions.

Revision #3
Created 2026-07-20 19:24:10 UTC by Dennis Underwood
Updated 2026-07-21 19:32:25 UTC by Dennis Underwood