

Wie schützt Cyber Crucible Fertigungs-, OT- und ICS-Umgebungen?

Kurzantwort: Die Lösung läuft vollständig auf dem Endpunkt ohne Cloud-Abhängigkeit und schützt so operative Technologien und industrielle Steuerungssysteme, die offline, luftisoliert (air-gapped) oder nur zeitweise verbunden sind — und sie unterbricht ausschließlich den bösartigen Prozess, sodass die Produktion weiterläuft.

Warum herkömmliche Tools hier an ihre Grenzen stoßen

OT- und ICS-Umgebungen können weder einen Cloud-Umweg noch eine vollständige Netzwerkspernung tolerieren. Viele sind bewusst getrennt vom Netz. Sicherheitsmodelle, die von ständiger Konnektivität und einem entfernten SOC ausgehen, greifen hier schlicht nicht.

Was sich ändert

- **100 % offlinefähig** — vollständiger Schutz ohne erforderliches Signal, bereit für den Air-Gap-Einsatz.
- **Keine Systemsperrungen** — bösartige Prozesse werden im Arbeitsspeicher unterbrochen, während die Produktion weiterläuft.
- **Ein Agent für die gesamte Umgebung** — derselbe schlanke Agent schützt SPS-Steuerungen auf dem Werksboden, Fahrzeuge in einem Logistiknetzwerk und Schiffe auf See, ganz ohne Analysten im Prozess und ohne Annahmen zur Konnektivität.

Revision #1

Created 2026-07-24 04:38:46 UTC by Dennis Underwood

Updated 2026-07-24 04:38:46 UTC by Dennis Underwood