# Wo werden die Daten von Cyber Crucible verarbeitet — werden sie in der Cloud gespeichert?

**Kurze Antwort:** Bedrohungsanalyse und -reaktion erfolgen lokal auf dem Endpunkt, nicht in der Cloud. Cyber Crucible sammelt keine Kundendateien, Anmeldedaten oder Schlüssel und speichert keine Kundeninhalte bei einem Drittanbieter-Public-Cloud-Dienst. Das Management- und Reporting-Backend läuft auf von Cyber Crucible betriebener Infrastruktur in den Vereinigten Staaten, und für Organisationen, die keinerlei externen Datenfluss zulassen dürfen, steht eine vollständig On-Premises- oder air-gapped-Bereitstellung zur Verfügung.

## Warum lokale Verarbeitung wichtig ist

- **Die Schutzentscheidung verlässt niemals das Gerät.** Detect–Decide–Respond läuft im Kernel auf dem Endpunkt, typischerweise in unter 200 Millisekunden, ohne dass im kritischen Pfad ein Umweg über die Cloud erfolgt.
- **Vom Backend unabhängiger Schutz.** Ein Ausfall des Management-Backends verringert nicht den Schutz des Endpunkts.
- **Wahlfreiheit bei der Bereitstellung.** Organisationen mit strengen Vorgaben zur Datenresidenz oder Datenhoheit können Cyber Crucible vollständig innerhalb ihrer eigenen gesicherten Infrastruktur betreiben.

## Worauf sich ein Prüfer verlassen kann

Da Kundeninhalte niemals erfasst werden, hat die Frage „Wohin gehen unsere Daten?" für die Kategorien mit dem höchsten Risiko eine einfache Antwort: Sie gehen nirgendwohin. Detaillierte Informationen zur Infrastruktur und zu Unterauftragsverarbeitern werden Prüfern unter NDA zur Verfügung gestellt.

---

Revision #1
Created 2026-07-24 04:51:52 UTC by Dennis Underwood
Updated 2026-07-24 04:51:52 UTC by Dennis Underwood