Does Cyber Crucible have a SOC 2 report?

Short answer: No. Cyber Crucible does not currently hold a SOC 2 attestation, and it says so plainly rather than implying otherwise. The reason is architectural: Cyber Crucible is a locally-executing software product, not a cloud custodian of customer data, so the SOC 2 service-organization model — which attests to how a provider stores, processes, and transmits *your* data on its own systems — does not map cleanly to it.

Why most customers have not required one

SOC 2 attests to the controls of a service organization that holds customer data. Cyber Crucible's design removes that premise:

- Threat detection and response run on the endpoint, at the kernel level, on the customer's own device.
- Customer files, credentials, encryption keys, and session tokens are never collected, transmitted, or stored by Cyber Crucible.
- The platform can be deployed fully on-premises or air-gapped, inside the customer's own infrastructure.

Because the highest-risk categories of data are never in Cyber Crucible's custody, a large part of the vendor-risk surface a SOC 2 is meant to address is removed by design rather than merely controlled.

What stands in its place

For reviewers who work from a questionnaire, Cyber Crucible provides a prepared vendor security package that supplies the underlying control evidence directly, and maps its controls to the SOC 2 Trust-Service Criteria and the NIST Cybersecurity Framework so a reviewer can complete a standard questionnaire from it. The package is available under a mutual NDA from **dpo@cybercrucible.com**.

The assurance roadmap is kept under evaluation against customer needs; this page will be updated if that position changes.

Revision #2
Created 2026-07-23 15:18:04 UTC by Dennis Underwood
Updated 2026-07-23 18:19:35 UTC by Dennis Underwood