Is Cyber Crucible FedRAMP authorized, and how does it serve government agencies?

Short answer: No — Cyber Crucible does not currently hold a FedRAMP authorization, and it does not imply otherwise. FedRAMP authorizes cloud service offerings that hold agency data; Cyber Crucible's model is different. It runs locally on the endpoint and can be deployed fully on-premises or air-gapped inside the agency's own boundary, so agency data never leaves that boundary for a third-party cloud.

How the architecture fits government

- **On-premises / air-gapped deployment.** The platform can run entirely within an agency's secured infrastructure, with no external data flow — suitable for classified, disconnected, and high-security environments.
- **No agency data collected.** Customer content, credentials, and keys are never collected, which removes much of what a cloud authorization is designed to protect.
- **US-made and export-controlled.** The software is subject to U.S. Department of Commerce EAR (not ITAR), and is internationally patented following USPTO review that included Department of Defense review.

The honest boundary

Where an agency requires a specific authorization (FedRAMP, StateRAMP), Cyber Crucible does not currently hold it; the on-premises deployment model is the path that keeps data inside the agency boundary. Deployment and control detail is provided under NDA.

Revision #2
Created 2026-07-23 15:18:23 UTC by Dennis Underwood
Updated 2026-07-23 18:19:53 UTC by Dennis Underwood