Cyber Crucible est-elle autorisée FedRAMP, et comment sert-elle les agences gouvernementales ?

Réponse courte : Non — Cyber Crucible ne détient actuellement aucune autorisation FedRAMP, et ne laisse entendre le contraire en aucune façon. FedRAMP autorise les offres de services cloud qui hébergent des données d'agences ; le modèle de Cyber Crucible est différent. Il s'exécute localement sur le terminal (endpoint) et peut être déployé entièrement sur site ou en environnement isolé (air-gapped) à l'intérieur du périmètre propre de l'agence, de sorte que les données de l'agence ne quittent jamais ce périmètre pour un cloud tiers.

En quoi l'architecture convient au secteur gouvernemental

- **Déploiement sur site / en environnement isolé.** La plateforme peut fonctionner entièrement au sein de l'infrastructure sécurisée d'une agence, sans aucun flux de données externe — adaptée aux environnements classifiés, déconnectés et à haute sécurité.
- **Aucune donnée d'agence collectée.** Le contenu client, les identifiants et les clés ne sont jamais collectés, ce qui élimine une grande partie de ce qu'une autorisation cloud est conçue pour protéger.
- **Fabriqué aux États-Unis et soumis au contrôle des exportations.** Le logiciel est soumis à la réglementation EAR (Export Administration Regulations) du Département du Commerce des États-Unis (et non à l'ITAR), et est breveté au niveau international suite à un examen de l'USPTO ayant inclus une revue par le Département de la Défense.

La limite énoncée en toute transparence

Lorsqu'une agence exige une autorisation spécifique (FedRAMP, StateRAMP), Cyber Crucible ne la détient pas actuellement ; le modèle de déploiement sur site est la voie qui permet de conserver les données à l'intérieur du périmètre de l'agence. Les détails relatifs au déploiement et au

contrôle sont fournis sous accord de non-divulgation (NDA).

Revision #1
Created 2026-07-24 07:14:40 UTC by Dennis Underwood
Updated 2026-07-24 07:14:40 UTC by Dennis Underwood