Où sont traitées les données de Cyber Crucible — sont-elles stockées dans le cloud ?

Réponse courte : L'analyse des menaces et la réponse s'effectuent localement sur le point de terminaison, et non dans le cloud. Cyber Crucible ne collecte pas les fichiers, identifiants ou clés des clients, et ne stocke pas le contenu des clients chez un fournisseur de cloud public tiers. Le backend de gestion et de reporting fonctionne sur une infrastructure exploitée par Cyber Crucible aux États-Unis, et un déploiement entièrement sur site ou isolé (air-gapped) est disponible pour les organisations nécessitant un flux de données externe nul.

Pourquoi le traitement local est important

- **La décision de protection ne quitte jamais l'appareil.** Detect-Decide-Respond s'exécute dans le noyau sur le point de terminaison, généralement en moins de 200 millisecondes, sans aller-retour vers le cloud dans le chemin critique.
- **Protection indépendante du backend.** Une panne du backend de gestion ne réduit pas la protection du point de terminaison.
- **Choix de déploiement.** Les organisations soumises à des exigences strictes de résidence ou de souveraineté des données peuvent exploiter Cyber Crucible entièrement au sein de leur propre infrastructure sécurisée.

Ce sur quoi un évaluateur peut s'appuyer

Étant donné que le contenu des clients n'est jamais collecté, la question « où vont nos données ? » a une réponse simple pour les catégories les plus à risque : elles ne vont nulle part. Des informations détaillées sur l'infrastructure et les sous-traitants sont fournies aux évaluateurs sous accord de confidentialité (NDA).

Revision #1
Created 2026-07-24 07:13:08 UTC by Dennis Underwood
Updated 2026-07-24 07:13:08 UTC by Dennis Underwood