

¿Dónde se procesan los datos de Cyber Crucible? ¿Se almacenan en la nube?

Respuesta breve: El análisis de amenazas y la respuesta se realizan localmente en el endpoint, no en la nube. Cyber Crucible no recopila archivos, credenciales ni claves de los clientes, y no almacena contenido de los clientes con un proveedor de nube pública externo. El backend de gestión e informes se ejecuta en infraestructura operada por Cyber Crucible en Estados Unidos, y existe una implementación totalmente local (on-premises) o con air-gap disponible para las organizaciones que requieren un flujo de datos externo nulo.

Por qué importa el procesamiento local

- **La decisión de protección nunca sale del dispositivo.** Detect-Decide-Respond se ejecuta en el kernel del endpoint, típicamente en menos de 200 milisegundos, sin ida y vuelta a la nube en la ruta crítica.
- **Protección independiente del backend.** Una interrupción del backend de gestión no reduce la protección del endpoint.
- **Opción de implementación.** Las organizaciones con mandatos estrictos de residencia o soberanía de datos pueden ejecutar Cyber Crucible completamente dentro de su propia infraestructura protegida.

En qué puede confiar un revisor

Dado que el contenido de los clientes nunca se recopila, la pregunta "¿adónde van nuestros datos?" tiene una respuesta simple para las categorías de mayor riesgo: no van a ningún lado. La información detallada sobre la infraestructura y los subprocesadores se proporciona a los revisores bajo un acuerdo de confidencialidad (NDA).

Revision #1

Created 2026-07-24 02:02:58 UTC by Dennis Underwood

Updated 2026-07-24 02:02:58 UTC by Dennis Underwood