

¿Dónde se procesan mis datos y pueden permanecer dentro de mi país?

Respuesta breve: Sí. La infraestructura de Cyber Crucible puede configurarse de modo que el procesamiento se realice geográficamente cerca de su jurisdicción legal o dentro de ella, y una implementación totalmente local con air-gap mantiene todo dentro del límite de su propia red, sin telemetría saliente.

Configuración soberana

La infraestructura puede posicionarse para mantener el procesamiento dentro de la jurisdicción legal del cliente, o geográficamente cerca de ella. Esto está diseñado para respaldar el cumplimiento de los mandatos de residencia de datos, incluidos el Reglamento General de Protección de Datos de la UE (GDPR), la Ley de Protección de Datos Personales de Arabia Saudita (PDPL), el Decreto-Ley Federal N.º 45/2021 de los EAU y la Ley de Protección de Datos de Kenia.

La opción más sólida

Para las organizaciones que requieren un aislamiento total, el modelo local ejecuta todo el software de gestión backend dentro de sus propios racks de servidores físicamente protegidos. Cero telemetría y cero datos salen del límite de su red soberana.

Dado que la evaluación de amenazas y la interdicción de procesos ocurren localmente en el endpoint, típicamente en menos de 200 milisegundos, la protección no depende de ninguna conexión externa. La soberanía no tiene ningún costo en capacidad defensiva.

“Vea también: *“¿Qué modelos de implementación están disponibles para la soberanía de datos?”*”