¿Qué modelos de implementación están disponibles para la soberanía de datos?

Respuesta breve: Dos. Un modelo local totalmente aislado (air-gapped), en el que nada sale de su red, y un modelo alojado o híbrido asistido por la nube, con comunicaciones TLS cifradas mediante JWE hacia servidores organizados regionalmente. Ambos ofrecen la misma prevención local en menos de 200 milisegundos.

Comparación

	Soberano en las instalaciones (Air-Gapped)	**Alojado / Híbrido asistido por la nube**
Límite de tránsito de datos	100% contenido dentro de los racks de servidores físicamente asegurados del cliente	Comunicaciones TLS cifradas mediante JWE hacia servidores de aplicaciones regionales
Flujo transfronterizo	Ningún flujo de red externo; cero telemetría saliente	Organización geográficamente localizada para cumplir con los límites regionales
Alineación normativa	Compatible con requisitos estrictos de residencia y soberanía de datos nacionales	Diseñado para alinearse con directivas globales de privacidad (GDPR, PDPL, entre otras)

Cómo elegir entre ellos

El modelo air-gapped es adecuado para el gobierno, la defensa, la infraestructura crítica y cualquier organización sujeta a mandatos estrictos de residencia nacional o que opere en entornos desconectados.

El modelo híbrido es adecuado para organizaciones que desean una gestión centralizada y generación de informes en toda la flota, manteniendo al mismo tiempo los datos dentro de un límite regional.

La prevención es idéntica en ambos casos. El ciclo local Detect–Decide–Respond se ejecuta en el kernel del endpoint independientemente del modelo de implementación; la diferencia radica únicamente en dónde reside la infraestructura de gestión e informes.

Revision #1
Created 2026-07-24 01:55:40 UTC by Dennis Underwood
Updated 2026-07-24 01:55:40 UTC by Dennis Underwood