

Welche Bereitstellungsmodelle stehen für die Datensouveränität zur Verfügung?

Kurze Antwort: Zwei. Ein vollständig air-gapped On-Premises-Modell, bei dem keine Daten Ihr Netzwerk verlassen, und ein gehostetes oder hybrides Cloud-unterstütztes Modell mit JWE-verschlüsselter TLS-Kommunikation zu regional bereitgestellten Servern. Beide bieten dieselbe lokale Prävention in unter 200 Millisekunden.

Vergleich

	Souveräne On-Premises-Lösung (Air-Gapped)	Gehostet / Hybrid Cloud-unterstützt
Grenze der Datenübertragung	100 % innerhalb der physisch gesicherten Serverracks des Kunden enthalten	JWE-verschlüsselte TLS-Kommunikation zu regionalen Anwendungsservern
Grenzüberschreitender Datenfluss	Kein externer Netzwerkverkehr; keine ausgehende Telemetrie	Geografisch lokalisiertes Staging zur Einhaltung regionaler Grenzen
Regulatorische Ausrichtung	Unterstützt strenge nationale Anforderungen an Datenresidenz und -souveränität	Ausgelegt auf die Übereinstimmung mit globalen Datenschutzrichtlinien (GDPR, PDPL und andere)

Die richtige Wahl treffen

Das air-gapped Modell eignet sich für Behörden, Verteidigung, kritische Infrastrukturen und jede Organisation, die strengen nationalen Residenzvorgaben unterliegt oder in getrennten (disconnected) Umgebungen arbeitet.

Das Hybridmodell eignet sich für Organisationen, die eine zentrale Verwaltung und ein flottenübergreifendes Reporting wünschen, während die Daten dennoch innerhalb einer regionalen Grenze verbleiben.

Die Prävention ist in beiden Fällen identisch. Die lokale Detect-Decide-Respond-Schleife läuft unabhängig vom Bereitstellungsmodell im Kernel auf dem Endpunkt — der einzige Unterschied besteht darin, wo die Management- und Reporting-Infrastruktur angesiedelt ist.

Revision #1

Created 2026-07-24 04:42:54 UTC by Dennis Underwood

Updated 2026-07-24 04:42:54 UTC by Dennis Underwood