Quels modèles de déploiement sont disponibles pour la souveraineté des données ?

Réponse brève : Deux. Un modèle sur site entièrement isolé (air-gapped) où aucune donnée ne quitte votre réseau, et un modèle hébergé ou hybride assisté par le cloud avec des communications TLS chiffrées JWE vers des serveurs déployés régionalement. Les deux offrent la même prévention locale en moins de 200 millisecondes.

Comparaison

	Sur site souverain (isolé/air-gapped)	**Hébergé / Hybride assisté par le cloud**
Périmètre de transit des données	Contenu à 100 % au sein des racks de serveurs physiquement sécurisés du client	Communications TLS chiffrées JWE vers des serveurs d'application régionaux
Flux transfrontalier	Aucun flux réseau externe ; aucune télémétrie sortante	Mise en scène géographiquement localisée pour correspondre aux frontières régionales
Conformité réglementaire	Prend en charge les exigences strictes de résidence et de souveraineté nationale des données	Conçu pour s'aligner sur les directives mondiales en matière de confidentialité (GDPR, PDPL, et autres)

Comment choisir entre les deux

Le modèle isolé (air-gapped) convient aux administrations publiques, à la défense, aux infrastructures critiques et à toute organisation soumise à des mandats stricts de résidence nationale ou opérant dans des environnements déconnectés.

Le modèle hybride convient aux organisations qui souhaitent une gestion centralisée et des rapports à l'échelle de l'ensemble du parc tout en conservant les données dans un périmètre régional.

La prévention est identique dans les deux cas. La boucle locale Detect-Decide-Respond s'exécute dans le noyau au niveau du point de terminaison, quel que soit le modèle de déploiement — seule diffère la localisation de l'infrastructure de gestion et de reporting.

Revision #1
Created 2026-07-24 07:04:58 UTC by Dennis Underwood
Updated 2026-07-24 07:04:58 UTC by Dennis Underwood