



XQ SOVEREIGN DATA GOVERNANCE

Sovereign Data Capability

EXECUTIVE SUMMARY

Data sovereignty is a first-order priority globally. As nations diversify their economies, adopt artificial intelligence at scale, and treat critical infrastructure as a matter of national security, keeping data access and control local has become essential — it ensures compliance with national law, reduces exposure to external interference, and supports the growth of an indigenous technology sector, all while continuing to leverage global hyperscale infrastructure rather than replacing it.

Not a compliance exercise — control. Two separate exposures exist today: technically, a provider using standard architecture retains the capability to access data it stores; Legally, a provider may be compelled by its home country to provide access to customer data, regardless of where that data is stored. Data residency alone does not eliminate this exposure. Clients require data control: no third party should have technical or legal access to its data without explicit authorization.

XQ Sovereign Data Governance is the cryptographic layer that binds sovereignty to the data object itself — not the infrastructure perimeter. This means that exclusive key control and policy enforcement persists for data on AWS services, compute, and storage.

Two deployment options depending on requirements: 1. XQ Zero Trust Data Platform is deployed directly into AWS infrastructure in region; 2. XQ Zero Trust Data Platform is deployed on-prem in region and links to cloud data to remotely enforce data sovereignty.

The selection between them is determined by scale, investment appetite, sovereignty requirements and existing facility infrastructure.

1. THE FUNDAMENTAL DISTINCTION

Conventional approaches to sovereign workloads anchor sovereignty to a physical perimeter or regional deployment: lock the compute into a certified environment, air-gap the network, and trust that physical isolation is sufficient. When the perimeter changes — when workloads migrate to the cloud, when data leaves the network, or when a vendor changes — the sovereignty question must be re-litigated.

XQ Sovereign Data Governance inverts this model. Cryptographic sovereignty is bound to the data and the model artifacts themselves. Exclusive key control means that no infrastructure provider, including AWS, has access to plaintext under any operating condition. The protected payload is the data— not the rack in which it executes.





Dimension	Infrastructure-First Approach	XQ Sovereign Data Governance
Sovereignty Anchor	Physical perimeter of the facility	Cryptographic key hierarchy bound to data
Vendor Access to Plaintext	Possible if vendor has facility or network access	Zero — customer-exclusive key control
Migration Continuity	Requires re-accreditation of new boundary	Keys follow data across any environment
Infrastructure Dependency	Tightly coupled to specific hardware or service	Vendor-neutral; operates on any certified compute
Protection on Migration	New boundary must be established	Continuous — same key architecture persists

2. XQ SOVEREIGN DATA GOVERNANCE: CORE CAPABILITY

XQ Sovereign Data Governance provides a Zero Trust Data Overlay (ZTDO) architecture that wraps cryptographic protection around data payloads at the object level.

Encryption keys and access policy are bound to the data itself — nothing leaves the environment until it is already secured, and control remains with the customer in region.

Access can be restricted to authorized users within the region regardless of where the underlying hardware is hosted, and every access — authorized or attempted — is independently logged in real time.

No party outside that key trust boundary — including AWS and any infrastructure operator — can access plaintext.

Capability Attribute	Description
Customer-Exclusive Key Control	Zero vendor access to plaintext under any operating condition. AWS does not hold, escrow, or have operational access to customer keys. This is enforced cryptographically, not by policy or contract.
Zero Trust Data Overlay (ZTDO)	Protection is bound to the data object, not the network perimeter. The payload remains protected whether at rest, in transit, or in use within an authorized processing environment.
Micro-Encryption	A unique encryption key is generated for every individual file, record, or artifact. Compromise of a single key exposes only that one object. The blast radius of any key compromise is mathematically contained.
Infrastructure-Neutral	Operates on customer-furnished hardware, on-premises infrastructure, or any other certified compute environment. The protection model does not change when the physical substrate changes.
Compliance Posture	DISA STIG compliant. NDAA Section 889 compliant. Post-quantum crypto-agile key management. Aligned with DoD Zero Trust Architecture target-level principles. Supports GDPR, NIS2, DORA, PIPEDA, Saudi & UAE PDPL, Australia Privacy Act, and other national sovereignty regulations.

3. XQ SOVEREIGN DATA GOVERNANCE ACROSS DEPLOYMENT OPTIONS

Regardless of which delivery path the customer selects, XQ Sovereign Data Governance provides the same sovereignty guarantees. The following capabilities are constant across Option A and Option B.





Capability	Option A — Cloud	Option B — On Prem + Cloud
Customer-Exclusive Key Control	Applied to all workload. AWS manages infrastructure; customer owns all keys.	On-prem keys and policies manage data in the cloud. Applied from point of encryption in region through transfer and inference. No vendor access at any phase.
Zero Trust Data Overlay (ZTDO)	Every data object (model artifact and inference output) bound to access policy. Wrong identity, wrong access level, wrong geolocation or wrong environment — decryption denied.	Cloud capabilities + on prem key and policy control which leashes access to data in cloud while retaining custody.
Micro-Encryption	Unique key per artifact. Single key compromise exposes only that object.	Unique key per artifact throughout all three transfer phases.
Data Migration	XQ key architecture migrates with the data. No re-accreditation of the cryptographic protection model required.	XQ key architecture migrates with the data. No re-accreditation of the cryptographic protection model required.

4. ARCHITECTURE: SOVEREIGN CONTROL PLANE

The diagrams below illustrates the sovereign control plane architecture operating inside AWS and the customer facility. The XQ cryptographic trust boundary is co-located with the accreditation boundary. Data sovereignty is maintained at the object level independent of the physical infrastructure layer. This architecture applies to both Option A and Option B — the difference between the options is the customer's regulatory need—not the underlying sovereignty model.

Option A - Cloud Only Deployment





Figure 1: XQ Sovereign Control Plane - AWS Deployment

Architecture Element Legend

Element	Description
XQ Cryptographic Trust Boundary	The primary sovereignty perimeter. Data objects — model artifacts, inference payloads, and output — are protected under customer-exclusive keys at this boundary. The boundary is cryptographic, not physical; it persists across facility or environment changes and migration.
Regional Boundary	Data Access is georestricted to the jurisdictional region. Attempts to access data outside the jurisdictional boundary are denied unless explicit permission is provided. Data access is controlled both within AWS and at the edge, across and beyond jurisdictional boundaries.
Operations Layer	The sovereign customer domain for workloads on AWS. XQ key control resides exclusively within this domain.

Option B - Hybrid Deployment

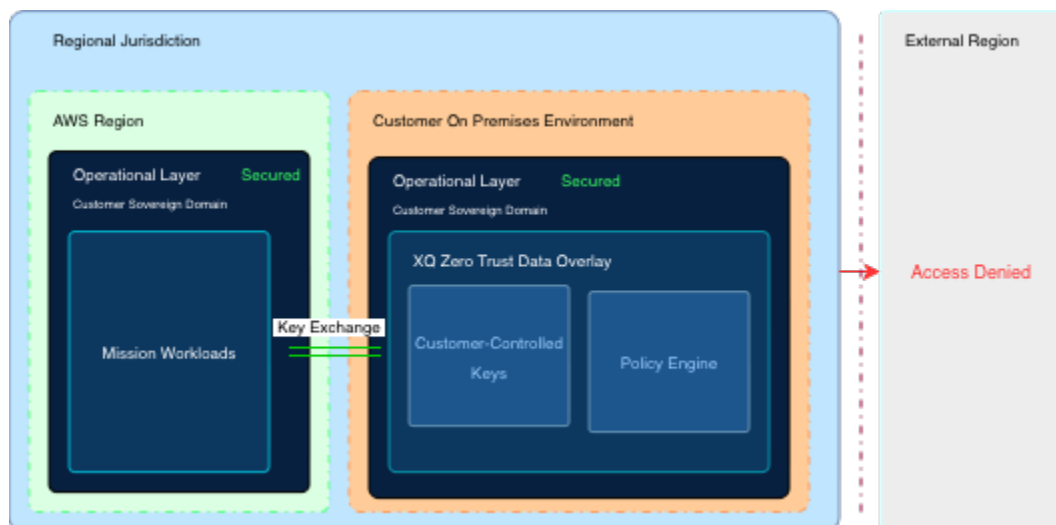




Figure 2: XQ Sovereign Control Plane - On-Prem + AWS Deployment

Architecture Element Legend

Element	Description
XQ Cryptographic Trust Boundary	The primary sovereignty perimeter. Data objects — model artifacts, inference payloads, and output — are protected under customer-exclusive keys at this boundary. The boundary is cryptographic, not physical; it persists across facility or environment changes and migration.
Regional Boundary	Data Access is georestricted to the jurisdictional region. Attempts to access data outside the jurisdictional boundary are denied unless explicit permission is provided. Data access is controlled both within AWS and at the edge, across and beyond jurisdictional boundaries.
Operations Layer	The sovereign customer domain for workloads. XQ encryption keys and policy engine resides within customer-owned, customer-operated, and customer-accredited independently. XQ key control extends to AWS cloud workloads.

5. STRATEGIC IMPERATIVE

The strategic imperative is to **decouple data sovereignty from cloud infrastructure location**. XQ enables AWS customers to keep using AWS's global cloud services while enforcing **where data can be accessed, where keys are held, and who can access it—within or outside a jurisdictional boundary**.

- **Maintain AWS agility:** Avoid creating separate sovereign cloud environments solely to satisfy data residency or sovereignty requirements.
- **Control data independently of AWS:** Apply persistent encryption, policy, RBAC/ABAC, and geofencing at the data layer.
- **Enforce jurisdictional boundaries:** Ensure data remains inaccessible when users, workloads, keys, or services operate outside approved jurisdictions.
- **Reduce regulatory and geopolitical risk:** Support requirements for data residency, localization, national control, and lawful access.
- **Enable cross-border operations:** Share and process data globally while maintaining jurisdiction-specific access policies.
- **Protect data across the lifecycle:** Maintain controls as data moves between AWS services, edge environments, SaaS applications, AI systems, and other clouds.





- **Avoid cloud lock-in:** Make sovereignty controls portable across AWS regions, clouds, edge infrastructure, and hybrid environments.

Strategic Position

1. XQ allows AWS customers to achieve data sovereignty at the data layer—not by restricting where they use the cloud, but by controlling where their data can be accessed, decrypted, and processed.
2. Cryptographic sovereignty maintained continuously from interim to permanent — no re-accreditation required.
3. A competitor that establishes sovereign mindshare during this window converts it into long-term platform lock-in. Both options close that window now.

6. SCOPE CLARIFICATION

XQ Sovereign Data Governance is not a network perimeter control. It does not substitute for facility accreditation or physical security controls. It operates as a complementary layer that ensures data sovereignty is maintained at the object level regardless of the physical environment — including in scenarios where the physical boundary is changed, extended, or migrated.

The commercial AWS services remain subject to standard AWS shared responsibility and data handling terms applicable to the commercial region. XQ cryptographic protection applied at the point of export ensures that no AI model artifact enters the environment without customer key coverage.

10. RECOMMENDED NEXT STEP

A 60-minute technical session is recommended to address the following in sequence:

1. Option qualification — Determine which delivery path aligns to the customer's scale, timeline, and facility readiness.
2. Key management architecture — How XQ customer-exclusive key control integrates with the customer's existing security posture and accreditation framework.





3. Workload integration — Specific workloads, models, frameworks, and inference patterns the customer intends to run.

