



Zero Trust Data Security

Govern. Safeguard. Oversee.

Zero Trust Data Center Security

Zero Trust Data Sovereignty: Total Control Beyond the Infrastructure

Granular Data Governance and Record-Level Sovereignty for Modern Data Centers

Challenges

Cloud services & apps expose critical data internally and externally with no audit trail of sharing, viewing, exfiltration or access location.

- 1. Cloud-to-Edge Control:**
 - Maintain absolute authority over your data as it travels anywhere—from centralized cloud environments directly to the tactical edge.
- 2. Infrastructure Security is Not Data Security:**
 - Relying solely on network perimeters or secure infrastructure leaves the actual data vulnerable once the perimeter is breached.
- 3. The Danger of Third-Party Trust:**
 - Organizations surrender control and invite breaches when they hand over data access to third-party platforms, apps, and identity services.
- 4. Vulnerabilities in Motion:**
 - When data is extracted, moved, or shared outside of secure enclaves (like Snowflake), it loses its native security measures and governance.
- 5. Blind Spots in Data Access:**
 - Traditional models offer no audit trail for who accessed or shared your data, making it impossible to track stolen information or enforce controls after it leaves your network.

XQ Solution

Automated cloud services for monitoring & external control of every data journey with zero trust data

- 1. Jurisdictional Geofencing:**
 - Ties decryption to approved physical locations. If data crosses sovereign borders, it cannot be decrypted.
- 2. Split-Knowledge Key Management:**
 - Separates encryption keys from the data. Neither the cloud provider nor XQ can Hi.access the plaintext data, preserving absolute sovereignty.
- 3. Forensic Chain of Custody:**
 - Delivers a record-level audit trail (who, when, and where data was accessed) to streamline compliance for CMMC, DFARS, and GDPR.
- 4. Cryptographic Erasure:**
 - Allows instant, remote revocation of encryption keys. In a breach, exfiltrated data immediately becomes unreadable "digital dust."
- 5. Granular Policy Enforcement**
 - Apply per-record ABAC and RBAC based access control



Control Over Sovereign Data, Anywhere It Goes

XQ's Zero Trust Data architecture elevates the sovereign data center by shifting protection from the physical perimeter directly to the data. This data-centric security layer enables secure interoperability and cross-domain collaboration without ever compromising jurisdictional boundaries. By wrapping every record in automated compliance, geographic access controls, and cryptographic self-protection, XQ ensures your information remains strictly sovereign—no matter where it is shared, moved, or stored.

»» Private Cloud Infrastructure. Total Independent Control.

XQ is a patented Zero Trust Data platform that separates infrastructure access from data access for each record. Even within a third-party private cloud, you maintain remote, cryptographic control and absolute visibility over who views your data and where.

»» Zero Trust AI Governance (AI DLP)

Safely deploy AI without risking data leakage or surrendering intellectual property. XQ applies Zero Trust Data Loss Prevention directly to the AI lifecycle—securing the user's prompt, cryptographically restricting the data the AI can reference, and governing the insights to ensure sovereign data is never exposed or absorbed into unauthorized models.

»» Secure Data Portability

XQ's automated external key control eliminates infrastructure lock-in. Seamlessly and securely move workloads between public, private, or sovereign cloud environments while maintaining strict, uninterrupted cryptographic control and compliance.

