



External Security and Governance for Snowflake

Encrypt, Monitor and Control Data Access with External Control

Granular Data Governance and Record-Level Sovereignty

Challenges

Snowflake can expose critical data internally or externally without a complete audit trail of who shared, accessed, viewed, or exfiltrated the data.

Breaches Happen When Third Parties Get Data Access

Organizations lose control of sensitive data when they grant Snowflake, applications, and identity services access to their data.

Network Security & Governance Break Down

When data is moved into, out of, or shared through Snowflake, organizations can lose the ability to enforce security policies and maintain control over the data.

No Control Over Stolen or Shared Data

Once data is accessed, copied, or shared, organizations may lack a persistent record of who accessed it, where it went, or who it was shared with.

Governance & Compliance Complexity Slows Business

Stringent privacy and data sovereignty requirements make it increasingly difficult to govern data across global cloud environments and enforce data localization requirements.

The XQ Message Solution

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

Jurisdictional Geofencing

Ties decryption to approved physical locations. If data crosses sovereign borders, it cannot be decrypted.

External Record-Level Access Control

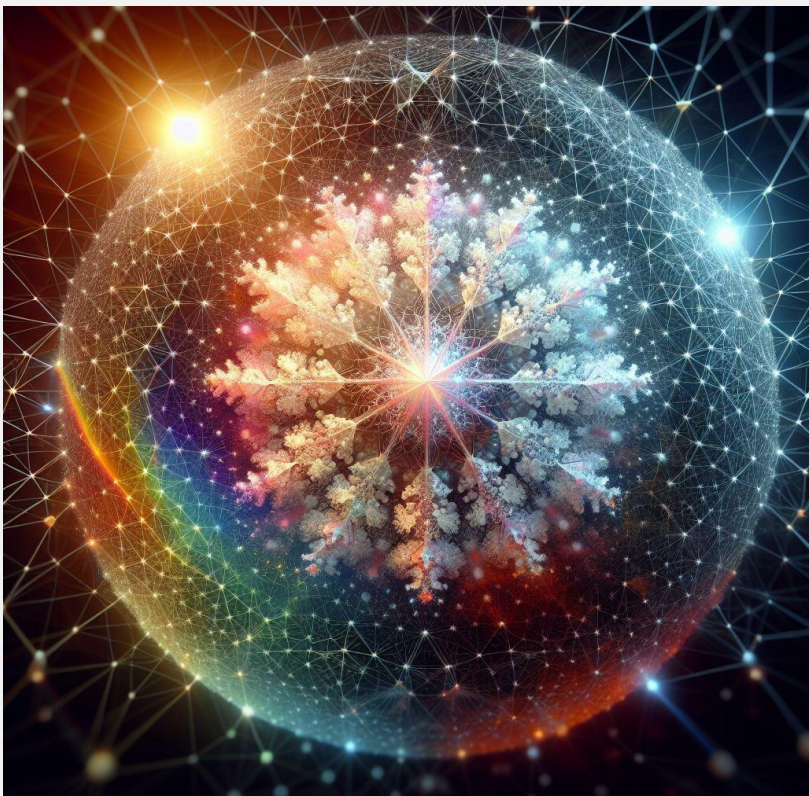
By separating data access from application and infrastructure access, XQ enforces persistent, RBAC and ABAC controls over data—regardless of where it resides.

Take Ransomware Extortion Off the Table

XQ can immediately revoke access to protected data even after data has been copied. This limits the value of stolen data and removes a lever of ransomware extortion.

Automated Governance & Compliance

Automated key and secrets management, data loss prevention, and policy enforcement create a persistent chain of custody for every data record, simplifying governance, auditing, and compliance.



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.



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.



Zero Trust Data Sharing

XQ is a **patented** Zero Trust Data Platform that separates network and application access from data access, letting you control and monitor who views your data remotely.