Zero Trust Data Vault

Cross-boundary DRM with secure file encapsulation and chain of custody.

Challenges

Data storage faces challenges with leakage, management overhead, access control and aging credential theft.

1. Centralized Responsibility Security Model
   - Data, secrets and policies are vulnerable in the same environment

2. Lack of chain of custody for data
   - Opens up customers to compliance violations

3. Environment-based data security and compliance
   - Data loses security and compliance when it is moved

4. Credential theft, ransomware exfiltration and aging tokens
   - Tokens and credentials can be hijacked to exfiltrate data

The **XQ Message** Solution

A cloud-based solution for zero trust data access (ZTDA) that encapsulates your data and delivers object level security.

1. Shared Responsibility Security Model
   - XQ's technology allows the customer to keep exclusive control of the encryption keys
2. Forensic level chain of custody and data sovereignty
   - A complete audit trail of every data object, is used to migrate, geofence, and protect data across disparate networks
3. Mitigates risks from misconfiguration or bad internal actors
   - Separates network access from data access
4. Dynamic credentialing mitigates risks from ransomware and insider threats and session token hijacking
   - Protection and control travel externally with the data to blow up exfiltrated data

Benefits

XQ Vault elevates your data storage to zero trust data access (ZTDA) by microsegmenting and encapsulating your data to control access both inside and outside your network, application or cloud.

⟫ Automated Secret Control

Minimize data and maintenance expenditures associated with secure data storage, while simultaneously enhancing security and bolstering auditability. Each file is protected with dynamic credentials and policies that are not tied to the AWS environment.

⟫ Zero Trust Sharing From Your Cloud

Data segmentation transforms Azure into a large and cost efficient zero trust storage service available, enabling compliance and sharing.

⟫ Compliance

XQ data rights management (DRM) crosses boundaries between environments and creates a unique secure chain of custody for each data object.

(Microsoft Partner) Contact : Brian Wane | brian@xqmsg.com

XQ Message
on Azure

XQ enhances Azure by providing secure data custody, geo-fencing, and access policy enforcement for data sovereignty from the edge to the cloud. This complements Azure Sovereign Cloud and simplifies compliance, aligning with the Shared Responsibility Security Model.

XQ also seamlessly integrates with Azure data storage services, enabling customers to maintain CMMC, GDPR, HIPAA, PCI, FERPA, and ITAR compliance on the Azure commercial cloud without migration.

Case Study:
McGrathNicol

⟫ Challenges

McGrathNicol is a premiere forensic accounting firm located in Australia. McGrath has remediated over 500 ransomware breaches in the last year alone. They recognized that much of their time was spent establishing a chain of custody and that if that was protected in real time the ransomware threat could be largely prevented.

⟫ Solution

XQ's Zero-Trust Vault solved several problems:
1. How to ensure duty of care and intake data compliantly and safely during a breach
2. Prepare clients to avoid a ransomware incident
3. Give clients the tools to protect their data and reduce the impact in the case of a breach

⟫ Results

XQ Vault has become the standard McGrathNicol uses to data intake from their clients. Additionally, it has become part of the recommended stack they advise their clients to use to prevent ransomware. Currently, no breaches from XQ protected data have been reported.
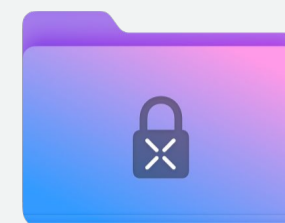
Features

Data Encapsulation

XQ microsegments and encrypts data, meticulously tracking and controlling access at every stage of data's journey beyond the boundaries of a single environment.

Remote Data Control

Turn exfiltrated data into digital dust by destroying or suspending keys.

Data Sovereignty

XQ data rights management (DRM) crosses boundaries between environments, enforcing jurisdictional policies and geofence data access.

Simple Compliance

XQ is built on the NIST standard and provides proof of secure chain of custody for each data object for global compliance standards.

Ransomware

Reduce your blast radius to one. Data access credentials are unique to each data object, stopping lateral data access.

Visit Azure Marketplace or XQ Message to purchase or start a Free Trial today. ⟫

Get started with XQ solutions on Azure