Zero Trust Data Email

Cross-boundary Data Right Management
with secure email encapsulation and chain of custody

Challenges

Email is the primary vector for cyberattacks and faces challenges with data leakage, insider threats, token high-jacking, phishing and credential theft.

1. Centralized Responsibility Security Model
   - Data rights are controlled by the email program
2. No chain of custody for data
   - Opens customer to compliance violations
3. Data access and application access joint hosted
   - Credentials give complete data access
4. Open to credential theft, ransomware, and man in the middle
   - Hijacking token and credentials to exfiltrate data

The XQ Message Solution

XQ Email is a cloud-based solution for zero trust data access (ZTDA) that encapsulates your data delivering unparalleled security and visibility for communications.

1. Shared Responsibility Security Model
   - XQ's Zero Trust Data technology allows the customer to keep exclusive control of the encryption keys & policies
2. Forensic level chain of custody and data sovereignty
   - With a complete audit trail of every data object, XQ can be used to geofence and protect data across disparate networks
3. Mitigates risks from misconfiguration or bad internal actors
   - Separates application access from data access
4. Mitigates risks from ransomware and phishing
   - External control with the data to blow up exfiltrated data

Benefits

XQ Email elevates your communications to zero trust data access (ZTDA) by microsegmenting and encapsulating your data to control access beyond the boundaries of a single environment.

Cross Platform Outlook, Gmail and Beyond

XQ's Zero Trust Data Protection keeps your Gmail and Outlook messages safe and reduces operational risks, without sacrificing collaboration.

Ransomware Extortion

XQ protects your data from double extortion, from phishing, credential theft, hijacked tokens and insider threats.

Compliance

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

XQ Message 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. 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: Blazar

Challenges

Blazar is a government RFQ aggregator that revolutionizes the procurement process by connecting multiple federal requirements with a portfolio of providers and manages the process from inception to completion. CMMC is a regulatory requirement federal contractors need to meet by 2024 to retain contracts.

Solution

XQ offers a way for organizations to achieve compliance with CMMC Level 2, which is a cybersecurity standard required for defense contractors. XQ secure email provides an alternative to moving to Gov Cloud and GCC HIgh, saving Blazar many thousands of dollars. Additionally XQ email protects against ransomware, phishing, and credential theft.

Results

XQ is game-changing solution for organizations in the defense industry that need to achieve CMMC compliance while using commercial cloud software and want robust data security and management features. XQ establishes a secure chain of custody for each email, which is vital for maintaining data integrity and traceability and the compliance required for CMMC level 2. Additionally, the inherent ransomware extortion protection make it a default choice for basic email security..

Features

Data Encapsulation

XQ microsegments and encrypts data during transfer, meticulously tracking and controlling access at every stage of data's journey.

Remote Data Control

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

Data Sovereignty

Data access controls (DAC) and Data Loss Prevention (DLP) policies enforce 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.

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

Get started with XQ solutions on Azure

XQ Message Contact : Brian Wane | brian@xqmsg.com