



XQ MESSAGE

XQ Message

Zero Trust Data Sovereignty

Securing and Classifying Data Everywhere

AWS Landing Zone Accelerator Integration



XQ's Capabilities Impact Critical Missions

Zero Trust Data Protection from Edge to Cloud

Ensures ITAR-controlled data is encrypted from the point of creation through cloud storage, preventing unauthorized access at any stage.

- XQ Secure Edge
- XQ Secure Application

Granular Access Controls and Policy Enforcement

Enforces ITAR access controls with policies tied to encryption keys, restricting access based on user roles, geolocation, and time-based conditions.

- XQ Platform

Cross-Border Audit Trail for Compliance and Forensics

Provides a tamper-proof audit trail of all data transactions, enabling organizations to demonstrate and enforce ITAR compliance and investigate potential breaches.

- XQ Platform

Secure Data Storage in Cloud Environments

Secures ITAR-controlled data stored in cloud environments like AWS S3 or databases with encryption and real-time access controls.

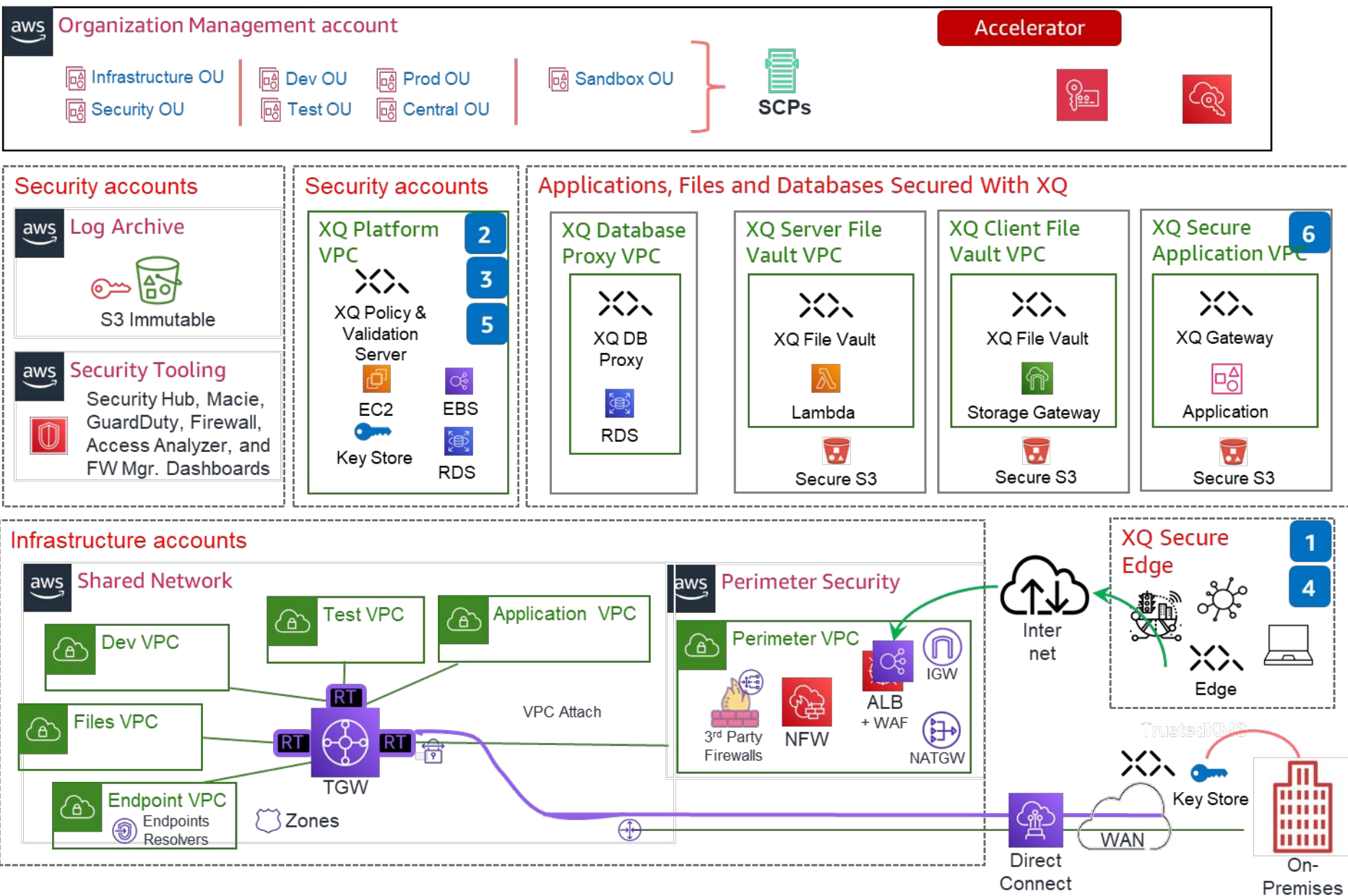
XQ Server File Vault
XQ Database Proxy

Minimal Infrastructure Changes

Integrates seamlessly with existing infrastructure to meet ITAR requirements without significant changes to IT environments.

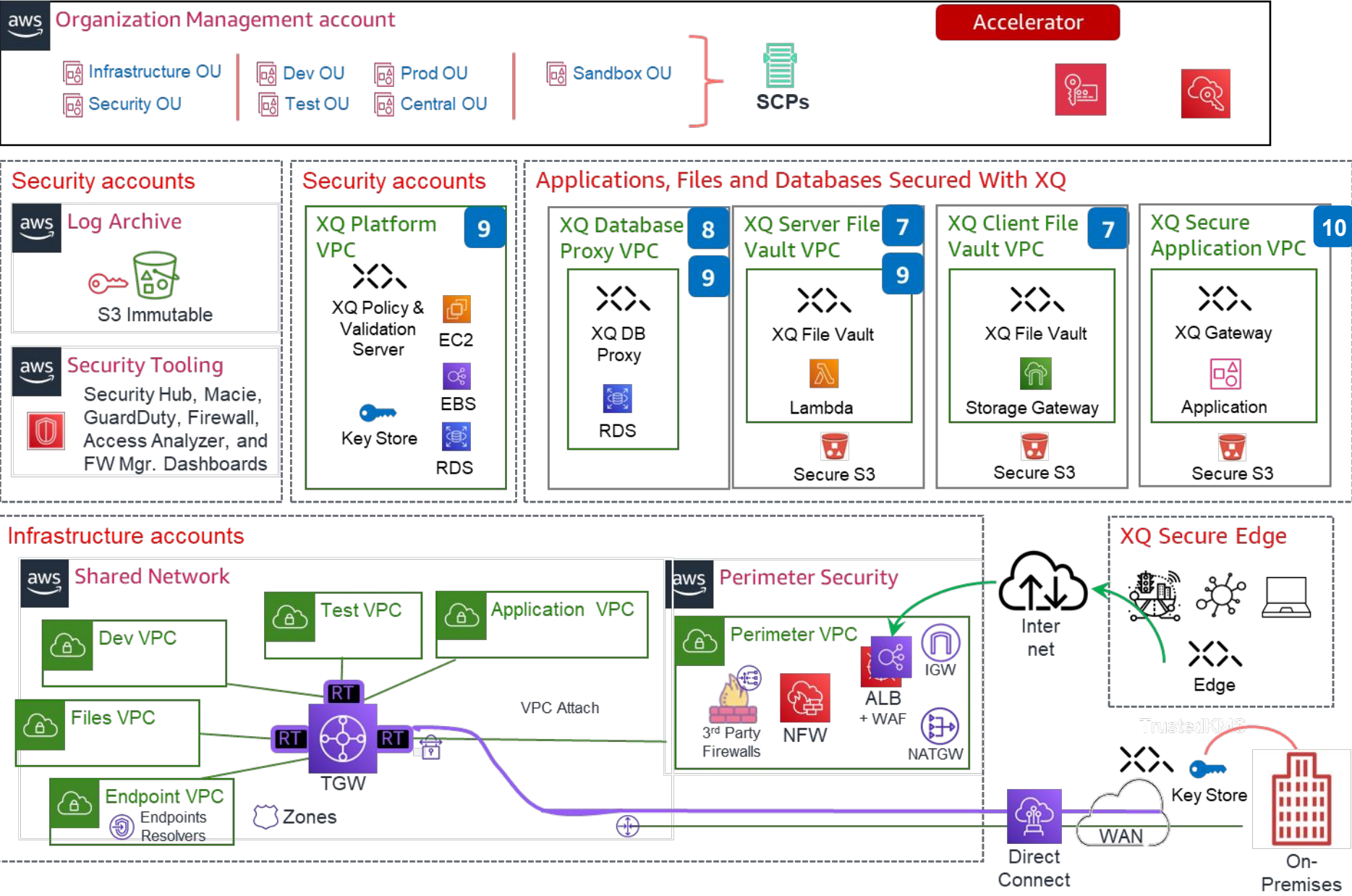
- XQ Platform's

XQ in TSE



- 1 Data Creation at the Edge Application**
 - Sensitive data is generated by an edge device or application (e.g., IoT sensor, XQ app, industrial system).
- 2 Authentication & Identity Verification**
 - The edge application authenticates with XQ using a trusted identity provider (e.g., OAuth, SAML, OpenID Connect) to verify the user, device, or system.
- 3 Key Generation & Policy Binding**
 - A unique, ephemeral encryption key is generated by the XQ platform and bound to a policy defining access controls, geolocation restrictions, time-based restrictions, and other conditions.
- 4 Local Encryption at the Edge**
 - The data is encrypted at the edge using the generated key and attached policy metadata, ensuring no unencrypted data enters the network.
- 5 Metadata Telemetry & Logging**
 - XQ logs metadata about the data transaction, including time of encryption, source device or user, policy attributes, and key custody chain.
- 6 Secure Transfer to AWS Cloud**
 - The encrypted data is transmitted over standard protocols (e.g., HTTPS, MQTT, REST) to an AWS cloud service (e.g., S3, Lambda, RDS, SQS).

XQ in TSE



- 7 File Storage in S3 (if applicable)**
 - Encrypted files are stored in S3 with encryption and access controls enforced by the XQ Server File Vault or XQ Client File Vault.
- 8 Database Storage (if applicable)**
 - Encrypted data is stored in a database with row-level encryption and access controls enforced by the XQ Database Proxy.
- 9 Policy Enforcement & Decryption (if Authorized)**
 - When the data is accessed in the cloud, the system requesting access must authenticate with XQ. XQ verifies the policy conditions in real time and releases the key for decryption if authorized.
- 10 ITAR Compatible Data Transfer**
 - XQ enables secure, compliant data transfer between applications within isolated VPCs, ensuring end-to-end encryption and external key control for ITAR-regulated environments.

Preventing access to ITAR data by third parties

AWS

With AWS Nitro based instances access is denied to the following:

- No Access to Memory/CPU State
- No insight into application processes
- No visibility of data in transit between hosts
- No access to customer-managed keys [e.g.; KMS, XQ]
 - Can not decrypt customer data

XQ

- No access to user encryption keys
- No access to decrypted data
- Cannot modify user permissions
- Cannot modify security policies
- No visibility into file/message content

Users

- No access to other users' data without explicit sharing permissions
- Cannot alter system security policies
- Cannot alter encryption protocols
- Cannot view audit logs
- Cannot view audit logs admin-level configuration settings



XQ MESSAGE

XQ Message

Zero Trust Data Governance

Securing and Classifying Data Everywhere

AWS TSE Integration