



Zero Trust Data Governance for Agents



Customer Scenario: Agentic Data Governance

Enhanced Data Security , Trust & Auditability

Challenge

Sensitive data and insights are difficult to classify, govern, and protect across cloud, edge, and AI environments.

Solution

XQ Agentic Data Governance will automatically discover, classify, encrypt, and enforce Zero Trust policies on data.

Immutable chain of custody.

Real-time monitoring and enforcement of contextual data access.

Benefits

- Automates governance
- Reduces compliance risk
- Secures AI and sensitive data
- Lowers operational effort
- Provides continuous audit visibility



Automated Data Governance No Matter Where Your Data Lives



XQ eliminates reliance on perimeter-based controls, encrypting and enforcing policies directly at the data level rather than focusing solely on network and endpoint restrictions.

Redefining Data Loss Prevention with Zero Trust Data Security

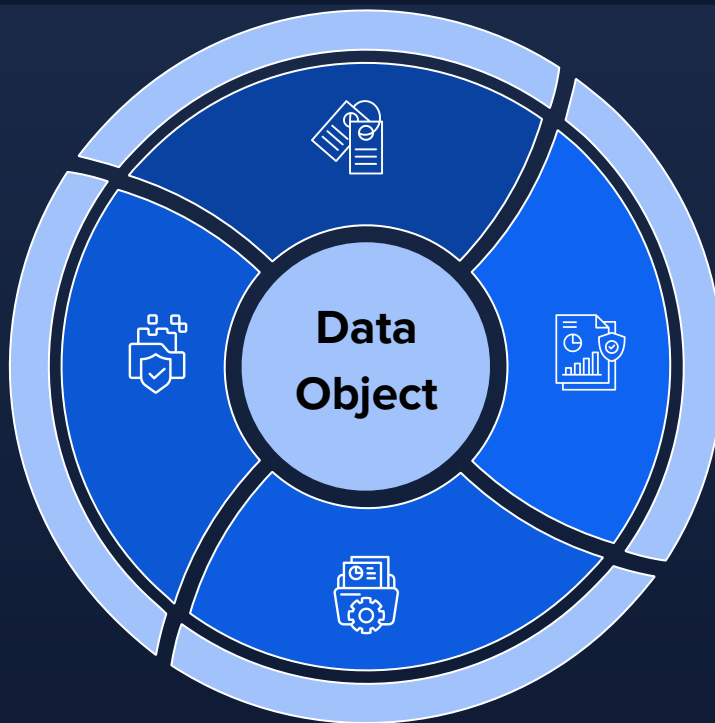


Object-Level Precision Defense

1. Labels & Categorization
2. Individual Encryption Key
3. IDP ABAC
4. Data ABAC
5. RBAC
6. Geography-Based Access
7. Chain of Custody
8. Remote Data Control

Data is not a byproduct of zero trust—
it is a primary control surface.

Data Loss Prevention with Data Centric Security



Lifecycle Governance

Ensures confidentiality, integrity, and availability regardless of where the data is stored or transmitted.

Attribute-Based Control

Governs access based on dynamic attributes of the user, data, and environment.

Object-Level Enforcement

Enforces granular controls directly on each data object

Cryptographic Binding

Binds policy and metadata directly to the data via encryption.

Zero Trust Data Pillar

XQ Capabilities



Enterprise
Data
Governance



Data Catalog
Risk
Alignment



Data Labeling
and Tagging



Data
Access
Control



Data
Monitoring
and
Sensing



Data Loss
Prevention



Data Encryption and
Rights Management

1. Control Over The Location of Your Data
2. Verifiable Control Over Data Access
3. The Ability to Encrypt Everything Everywhere
4. Data Resilience From The Edge To The Cloud
5. Automated Data Classification
6. Automated Role Based Access Control
7. Automated Data Governance and Loss Prevention



XQ & AWS ZTAG - Elevate Existing Environments to ZT Compliance

AWS Zero Trust Accelerator for Government

ZTAG-1 Zero Trust Reference Architecture

Aligns with US federal Zero Trust guidance

Modular, component based design with validated AWS Partners



Okta

Identity provider, MFA, RBAC, PEP and Identity store source of truth

CrowdStrike

Device signal; tracking non-person entity behaviors; Creating ZTA scores

AWS

Architectural security best practices
Managed services, SCP

XQ Message

Data rights management and data loss prevention; Distributed file encryption

Zscaler

Least-privilege PEP; Network obfuscation
Application micro-segmentation

Splunk

SIEM, UBA, Threat detection, Custom dashboards, data correlation

Splunk

SOAR, Threat Containment, Remediation Automation, Time Based Actions

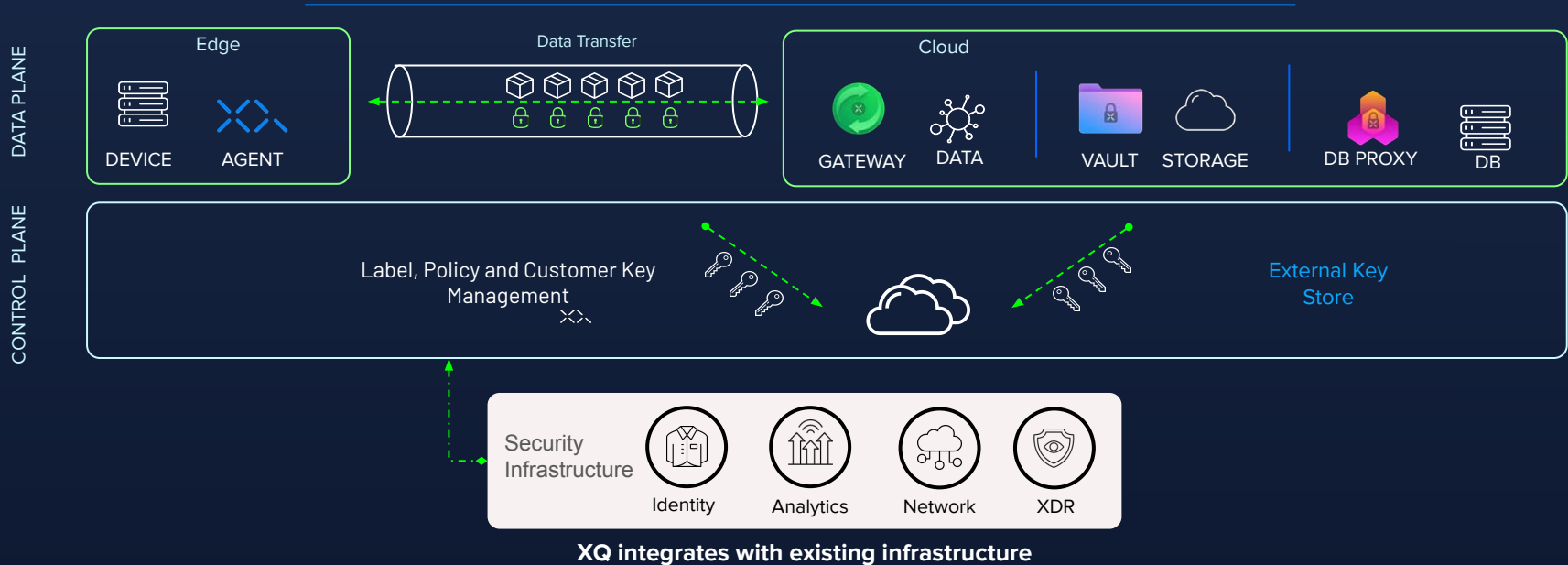
Partner Endorsement
AWS Zero Trust Accelerator for Government (ZTAG) is a program for federal agencies adopt zero trust security architectures

*Selected to meet the NIST / Zero Trust Data Requirements for the Data Pillar for AWS DoD Customers.

Govern Data From The Edge to Cloud

Unified monitoring and enforced access at the record level

Separation of data and control plane



Zero Trust Data Policy Enforcement Point Solutions



Database

Zero Trust Database



RDS, Snowflake & SQL



Transfer

Zero Trust Gateway

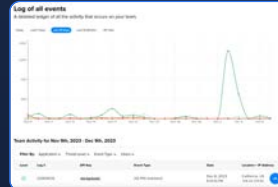


Migration & Web Gateway



API

Zero Trust API

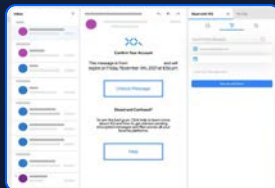


Application Integration



Email

Zero Trust Email



Outlook & Gmail



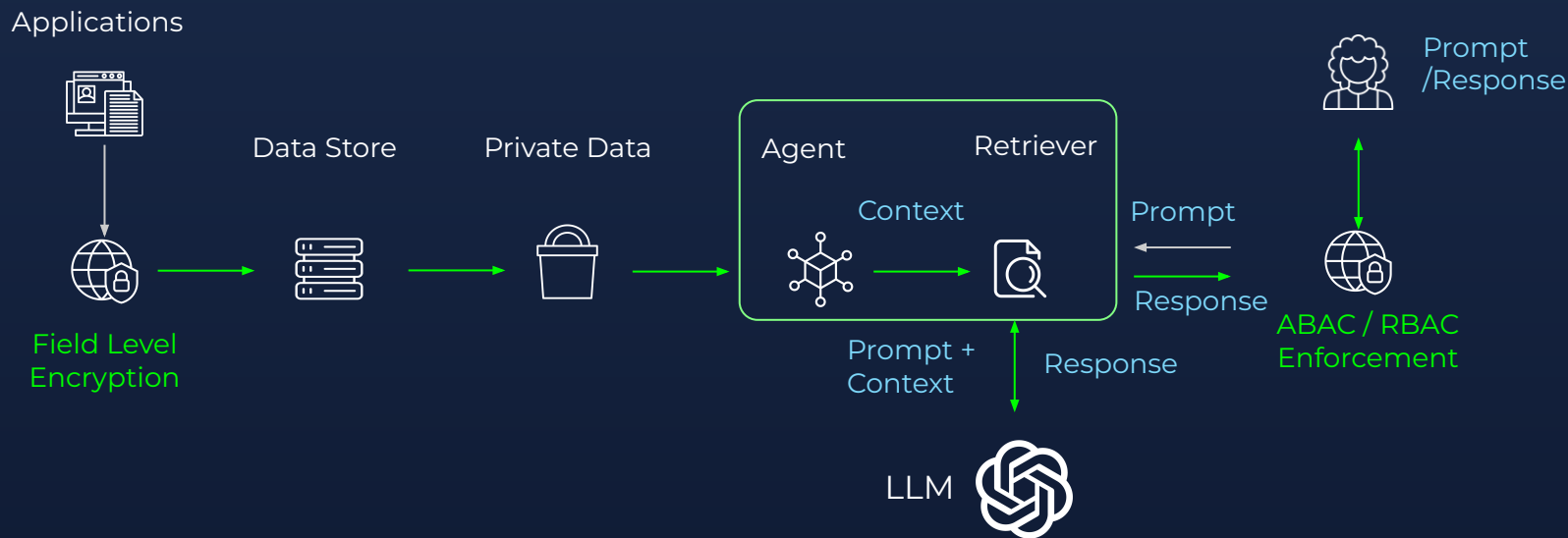
Vault

Zero Trust Files



One Drive, SharePoint

Zero Trust Data for Agents



■ XQ Protected

Sovereignty: Keep Data Control in Country

The only platform for ABAC driven data localization, residency and sovereignty in one



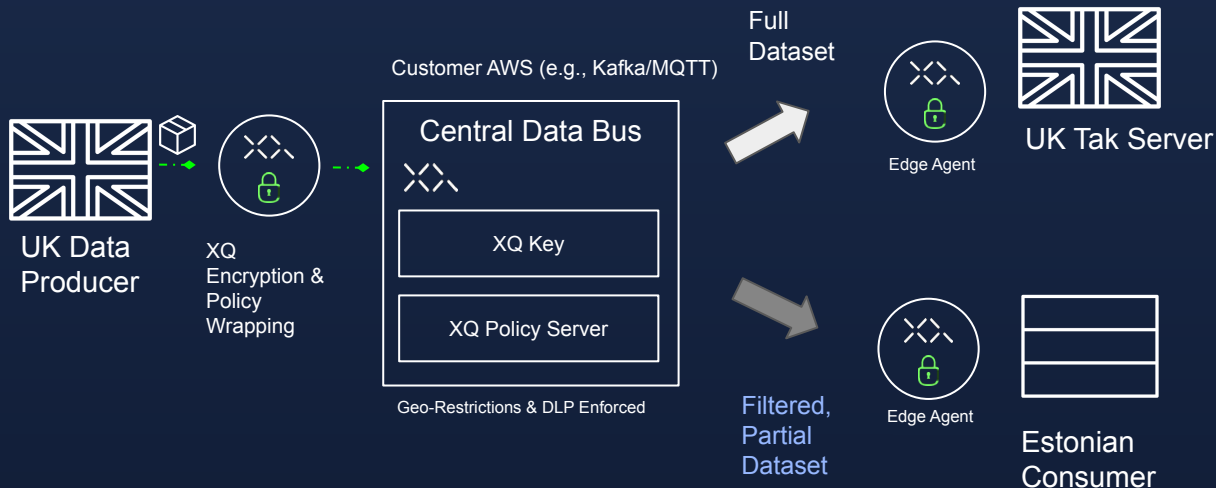
- ✓ Keep Data Access in Country
- ✓ Customer owned keys in country
- ✓ ACP 240,G DPR, DORA, NIS2, CMMC
- ✓ Audit trail from edge to cloud
- ✓ Data credentials stored in country
- ✗ Cloud provider access
- ✗ Third Party Data Access
- ✗ Data Exfiltration
- ✗ CLOUD ACT Access, SCHREMS 2 access



Coalition Sharing and Data Filtering

A Multi-Partner Data Sharing Model

Zero Trust,
ACP 240,
GDPR



1	Control (Metadata)	Attribute tagging & cryptographic binding
2	Protect (Access)	ABAC/RBAC + dynamic policy enforcement
3	Protect (Encryption)	Zero-knowledge encryption + control leash



XQ MESSAGE

XQ Message

Zero Trust Data Governance

Securing and Classifying Data Everywhere