DoD Zero Trust Strategy Review

DoD wants to ensure that frontline warfighters have access to data wherever and whenever they want!

POWERED BY

What is new:
- Data is being moved closer to warfighters - Mobile Data

Why is it important:
- Authorization now travels with the data to ensure access

XQ Message Value:
- First and only Zero Trust Data Protection solution with persistent policy enforcement for mobile data

Increasing Accessibility:
User Checks and Balances

Challenge: Warfighter interoperability and missions require a wide spectrum of partners, including DIB users, to access DoD networks safely and securely. Authorization to be on and authentication to get onto networks both need to occur. Simultaneously, DoD must institute safeguards to keep malicious actors out – whether state-sponsored seeking intellectual property or persons with malicious intentions.

Pre-ZT Architectures: Attempts to "lock-down" networks (e.g., from certain locations or time periods) and/or to overly restrict access to essential data (e.g., data base or file restrictions) hinder collaboration between DIB users. This increasingly occurs out of an abundance of caution to keep malicious actors out – and impacts interoperability at all mission levels.

Post-ZT Architectures: Adoption of a new, Zero Trust cybersecurity approach results in an effective set of checks and balances. DIB users located overseas and working outside "normal" business hours now can quickly gain authorization to access a sensitive network once they are authorized and authenticated successfully. This enables partners to access data WHEREVER and WHENEVER needed.

DoD Zero Trust Capabilities

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	2.1 Device Inventory	3.1 Application Inventory	4.1 Data Catalog Risk Assessment	5.1 Data Flow Mapping	6.1 Policy Decision Point (PDP) & Policy Orchestration	7.1 Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	2.2 Device Detection and Compliance	3.2 Secure Software Development & Integration	4.2 DoD Enterprise Data Governance	5.2 Software Defined Networking (SDN)	6.2 Critical Process Automation	7.2 Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	2.3 Device Authorization with Real Time Inspection	3.3 Software Risk Management	4.3 Data Labeling and Tagging	5.3 Macro Segmentation	6.3 Machine Learning	7.3 Common Security and Risk Analytics
1.4 Privileged Access Management	2.4 Remote Access	3.4 Resource Authorization & Integration	4.4 Data Monitoring and Sensing	5.4 Micro Segmentation	6.4 Artificial Intelligence	7.4 User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management	3.5 Continuous Monitoring and Ongoing Authorizations	4.5 Data Encryption & Rights Management		6.5 Security Orchestration, Automation & Response (SOAR)	7.5 Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		4.6 Data Loss Prevention (DLP)		6.6 API Standardization	7.6 Automated Dynamic Policies
1.7 Least Privileged Access	2.7 Endpoint & Extended Detection & Response (EDR & XDR)		4.7 Data Access Control		6.7 Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

| DoD Zero Trust Data Requirement	XQ Message Feature	Warfighter Benefit
4.1 Data Catalog Risk Assessment	Support of all data types in one platform	Multi-mission capability
4.2 DoD Enterprise Data Governance	One Dashboard to create and monitor policies	Simplified operations
4.3 Data Labeling & Tagging	Unique Meta Tag attached to every block of data	Easier application support
4.4 Data Monitoring & Sensing	Real Time Tracking of data location	Data exfiltration monitor
4.5 Data Encryption & Rights Management	Crypto agile encryption to match access policies	Improved system performance
4.6 Data Loss Prevention (DLP)	DLP content scanning for outbound Emails	Reduced data leakage
4.7 Data Access Control	Policy-based access to encryption keys	Coalition data sharing

Mobile Data Problem: Email, Files, IoT Data, Imaging . . . are on the move

Zero Trust Data Solution: Policy-based Key Distribution based on Geo-Location and Identity of software program requesting access

XQ enables warfighters to see where their data is & who is accessing it
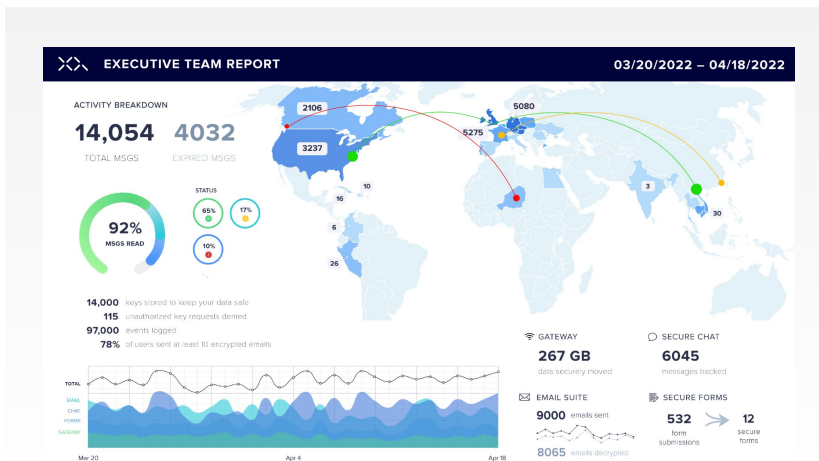
XQ's Zero Trust Data Protection

Secure Email & Files

IoT / Data Lakes
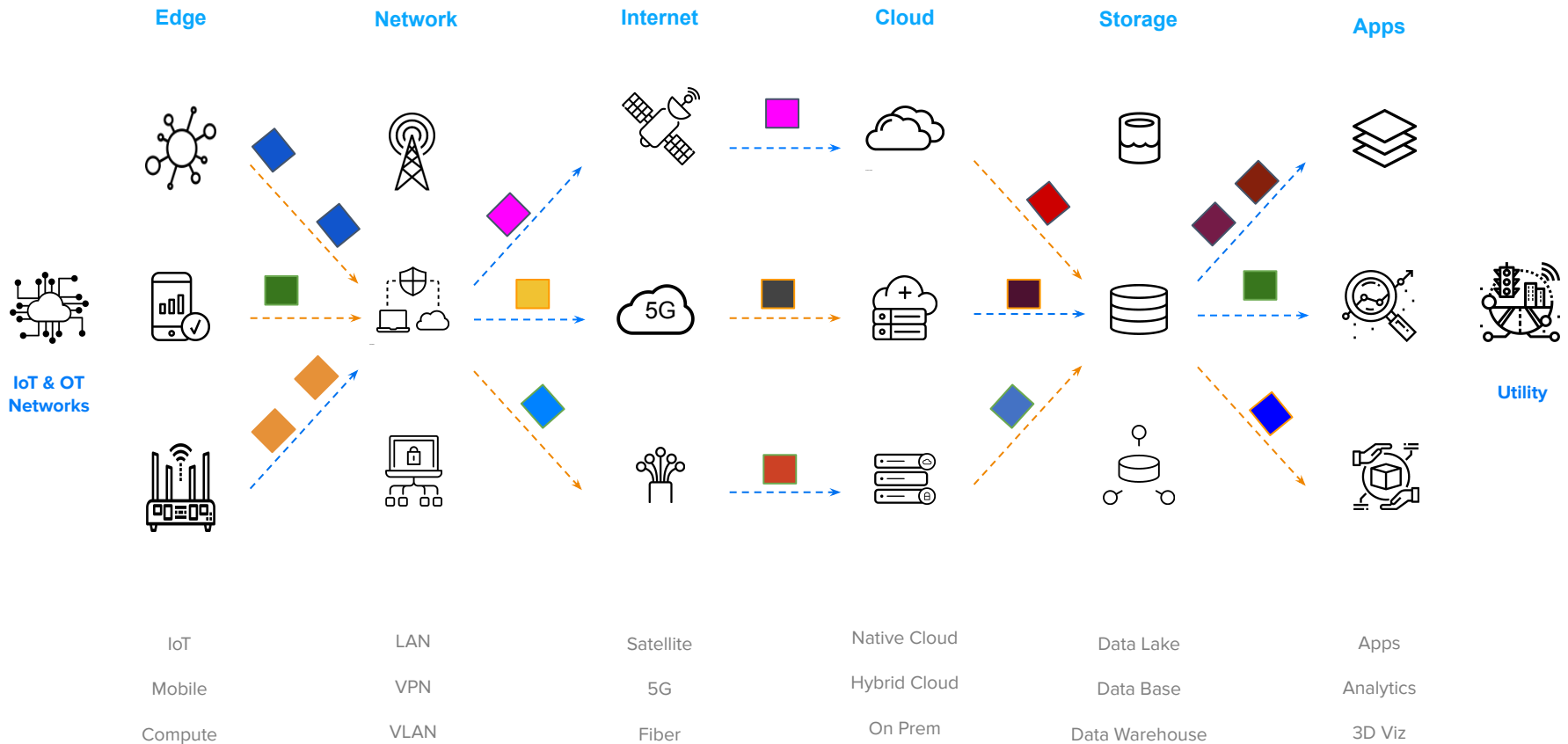
Secure Mobile 5G/Satellite Comms

VPN & MACsec replacement

Every Time Data Crosses A Network Boundary Or Is Stored In A Different Server The Encryption Key Is Changed

Edge	Network	Internet	Cloud	Storage	Apps
IoT	LAN	Satellite	Native Cloud	Data Lake	Apps
Mobile	VPN	5G	Hybrid Cloud	Data Base	Analytics
Compute	VLAN	Fiber	On Prem	Data Warehouse	3D Viz

IoT & OT Networks

Utility

Zero Trust Data Creates A Unique Meta-Tag Which Travels With The Data To Enable Persistent Policy Enforcement

Edge	Network	Internet	Cloud	Storage	Apps
IoT	LAN	Satellite	Native Cloud	Data Lake	Apps
Mobile	VPN	5G	Hybrid Cloud	Data Base	Analytics
Compute	VLAN	Fiber	On Prem	Data Warehouse	3D Viz

IoT & OT Networks

Utility

Zero Trust Data Gateway
Secure Data-in-Flight and At-Rest

Effortlessly transform your cloud data transfer workflow

XQ Gateway

XQ Gateway

S3

Azure aws

Azure aws

XQ Zero Trust Data Monitoring

The First Zero Trust Data Gateway

Secure hybrid cloud and S3 data transfer simplified

Full chain of custody to ensure data integrity and compliance

- **Every data object uniquely protected and tracked**

- **ITAR, CMMC, NIST-CUI, HIPAA, FINRA, ISO 270001**

Breakthrough Data Sharing Powered by Zero Trust Data Protection

S3 & Azure Blob Secure Cloud Storage
Every Bucket **is now a Zero Trust Vault**

Effortlessly transform your data storage workflow

Auto Encrypt

Auto Decrypt

S3

SFTP

SFTP

XQ Zero Trust Data Monitoring

Azure
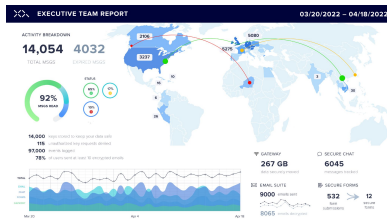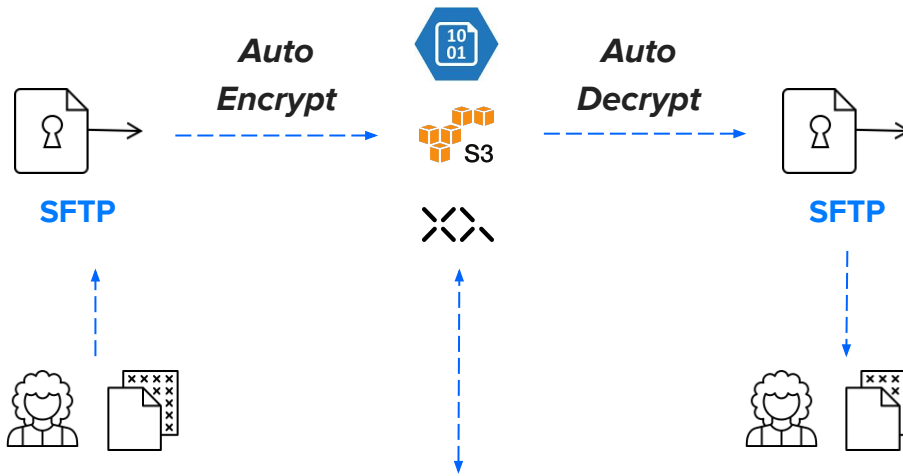
User friendly secure storage for infrastructure you control

Simplify your security and sharing

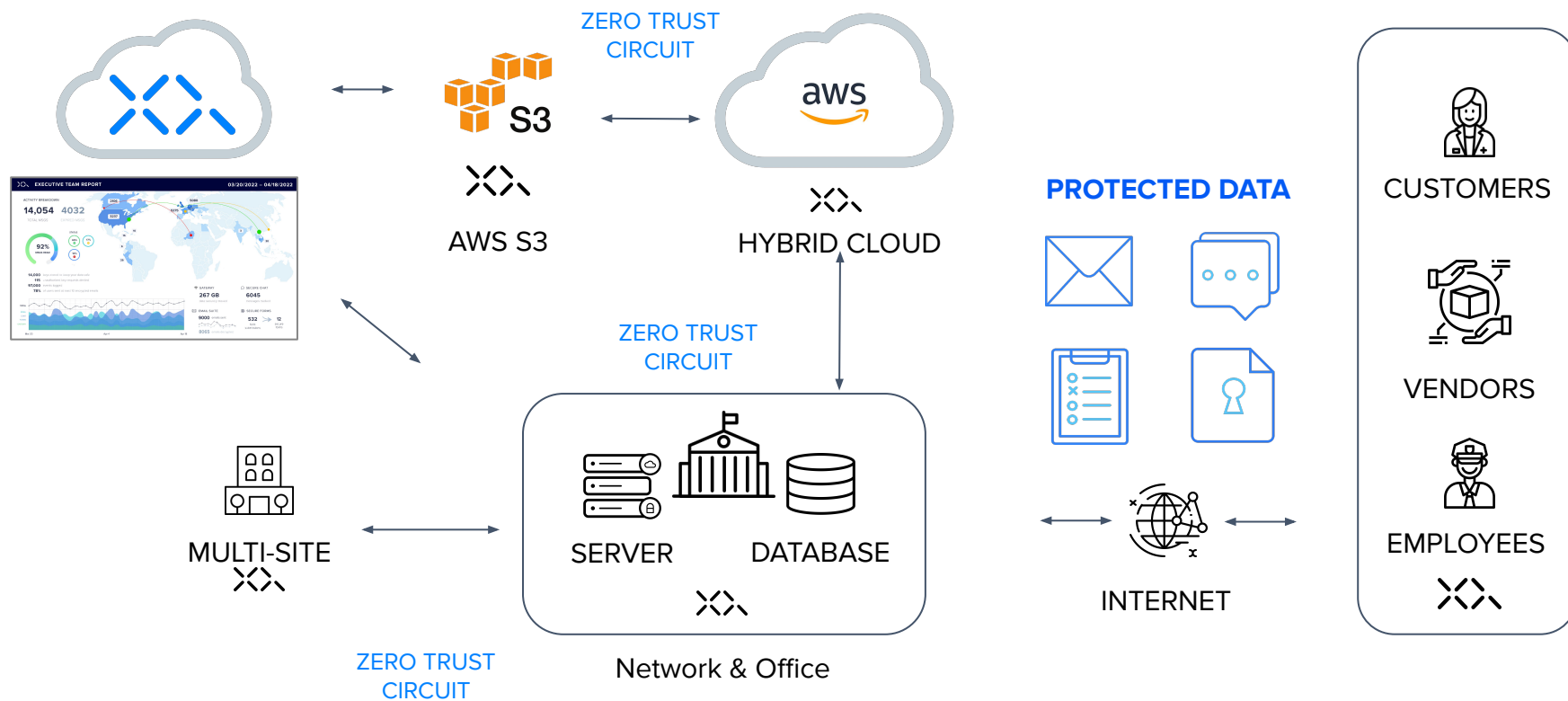**Full chain of custody to ensure data integrity and compliance**

- **Every data object uniquely protected and tracked**

- **ITAR, CMMC, NIST-CUI, HIPAA, FINRA, ISO 270001**

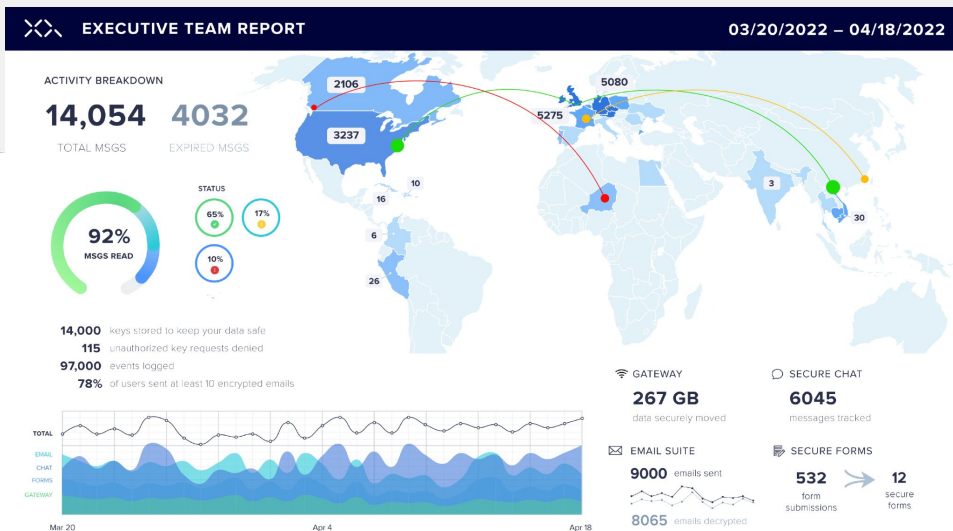Breakthrough Data Sharing Powered by Zero Trust Data Protection

XQ Seamlessly Protects CMMC Data Across Your Workspace

Full chain of custody to ensure data integrity and compliance.

ZERO TRUST CIRCUIT

AWS S3

HYBRID CLOUD

ZERO TRUST CIRCUIT

MULTI-SITE

SERVER   DATABASE

Network & Office

ZERO TRUST CIRCUIT

PROTECTED DATA

INTERNET

CUSTOMERS

VENDORS

EMPLOYEES

Thank You For Your Time

Contact XQ For Zero Trust Data Protection Demo or Trial Account

Junaid Islam
junaid@xqmsg.com

Randy Clark
randy@xqmsg.com