qanapi

Learn more at qanapi.com

AUGUST 2026

Meeting the federal Zero Trust mandate **at the data layer**

Why perimeter and identity controls alone cannot satisfy OMB M-22-09 — and how Qanapi closes the gap.

01 THE MANDATE

Executive Order 14028 and OMB Memorandum M-22-09 direct federal agencies toward Zero Trust Architecture (ZTA) across the five pillars defined in CISA's Zero Trust Maturity Model: Identity, Devices, Networks, Applications and Workloads, and Data. The technical foundation for this mandate is NIST Special Publication 800-207, *Zero Trust Architecture*, which defines ZTA as an enterprise security model built on continuous verification and resource-level protection rather than implicit trust based on network location. Agencies were required to meet baseline ZTA objectives by the end of FY2024. In May 2025, the Federal CDO and CISO Councils published the *Zero Trust Data Security Guide*, a formal M-22-09 deliverable confirming that the Data pillar, the hardest to operationalize, is now a required outcome, not an afterthought.

02 THE GAP

Most Zero Trust spending concentrates on Identity and Networks: multifactor authentication, micro-segmentation, and software-defined perimeters. These controls verify who is requesting access and from where, but once access is granted, the underlying data is unprotected. If a credential is phished, a workload is misconfigured, or CUI leaves the network boundary through email or a shared document, network and identity controls offer no further protection. Zero Trust that stops at the network edge is not Zero Trust for the data itself.

The Zero Trust mandate will not be satisfied by identity and network controls alone. Qanapi gives agencies and contractors verifiable, cryptographic control over the data itself, wherever it resides.

03 THE QANAPI SOLUTION — ZERO TRUST ENFORCED AT THE DATA LAYER WITH KARST

Qanapi's Karst platform and services map directly to all five ZTA pillars by enforcing protection on the data object itself, independent of network, device, or application:

IDENTITY	Object-level encryption ties decryption to verified user identity and role, enforcing continuous, per-access verification layered on top of existing identity providers, not a one-time login check.
DEVICES	Client-side encryption (CSE) ensures data is decrypted only on verified, managed endpoints; keys never reach unmanaged or unverified devices.
NETWORKS	Encryption travels with the data, not the network path. CUI remains protected in transit and at rest regardless of the network it crosses.
APPLICATIONS & WORKLOADS	The Karst Platform and Qanapi Flow integrate directly into digital workspaces and custom applications, enforcing protection at the moment of creation and use.
DATA · CORE PILLAR	Customer-held keys (Echo), object-level encryption, live redaction, and automated data lineage (Fathom) deliver the verifiable, auditable protection the Data pillar requires.

04 COMPLIANCE ALIGNMENT

Qanapi's Karst Platform is FIPS 140-3 validated, supporting AES-256 with post-quantum cryptographic options, and is built to align with NIST SP 800-207 Zero Trust Architecture principles. It aligns to NIST SP 800-53, FISMA, CMMC, HIPAA, CJIS, and ITAR requirements, and deploys platform integration in minutes, with no browser extensions and no added engineering burden.

NIST SP 800-53 · FISMA · CMMC · HIPAA · CJIS · ITAR

THE QANAPI PRODUCT FAMILY

- **Karst_Gorge** — Encryption API
- **Karst_Echo** — Key Management
- **Karst_Fathom** — AI Security
- **Qanapi_Flow** — Collaboration Security

Sources: OMB M-22-09 (Jan. 2022) · Executive Order 14028 · NIST SP 800-207, Zero Trust Architecture (Aug. 2020) · CISA Zero Trust Maturity Model v2.0 · Federal Zero Trust Data Security Guide (May 2025) · qanapi.com