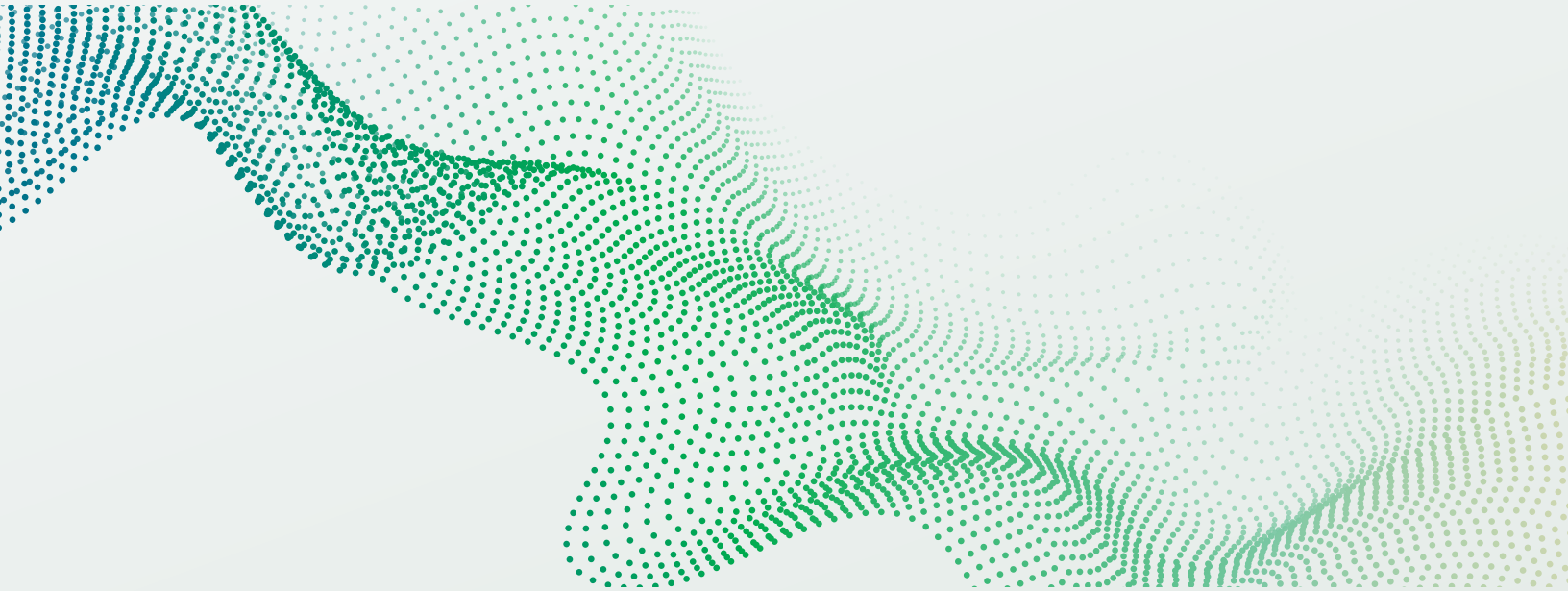
qanapi

WHITEPAPER

ZERO TRUST AT THE DATA LAYER

The Future of Zero Trust Architecture at the Data Layer

A Checklist to Simplify, Enhance, and Scale Data Security in 2026



THE ONLY API DELIVERING ZERO TRUST AT THE DATA LAYER

Zero Trust Architecture Is Evolving —Has Your System Kept Pace?

Zero Trust Security is firmly established as the most comprehensive and effective model for cybersecurity. Surveys show that **96%** of organizations favor Zero Trust and **81%** plan to implement it in 2026.[1]

But many security leaders are learning that standard Zero Trust architecture doesn't deliver the level of protection they need, especially with high-pressure AI mandates creating unprecedented new risks.

Without advanced post-quantum encryption (PQE) to secure sensitive data, companies cannot move forward safely within heavily regulated sectors. At the same time, leaders face a range of technical, cultural, and budgetary barriers. **58%** of organizations say their existing Zero Trust solution covers less than half of their business environment.[2] Equally, **62%** say Zero Trust will drive up their security costs,[3] and **41%** expect to add staff just to implement these solutions.[4]

This checklist will help you avoid these problems and implement Zero Trust 2.0. Use it to:

- Identify gaps in your existing data security program
- Deploy more robust and granular data security controls
- Reduce the cost and complexity—while making your system more flexible

THE CHECKLIST

Four Steps to Deliver True Zero Trust Protection

1 | Zero Trust 2.0 Security Foundations

ACTION	WHAT'S REQUIRED	NEED TO DO	DONE
Enforce explicit verification	Ensure every data access request is verified using identity tokens (JWTs) and access control lists, not just network perimeter security	☐	☐
Implement access controls at the data layer	Mandate "secure-by-design" access controls that exist at the data layer itself, not at the network or application level	☐	☐
Implement fine-grained access policies	Control access based on multiple factors: user identity, location, device type, and time of access	☐	☐
Deploy a "triangular" Zero Trust system	Combine identity verification, policy enforcement, and encryption in a unified approach	☐	☐
Separate authentication from data operations	Isolate token issuance from encryption/decryption processes to prevent credential exposure	☐	☐
Enable real time access revocation	Integrate with SIEM/SOAR systems through webhooks to dynamically enable or disable data access based on detected threats	☐	☐
Maintain audit trails for compliance	Ensure token lifecycle management and access events are logged for FedRAMP, CMMC, and defense regulatory requirements	☐	☐

2 | Optimize Architecture & Deployment

ACTION	WHAT'S REQUIRED	NEED TO DO	DONE
Implement cloud & on-prem agnostic architecture	Avoid vendor lock-in by using APIs that work consistently across any infrastructure	☐	☐
Optimize for low-latency performance	Leverage Redis-powered token caching to ensure sub-millisecond access control decisions	☐	☐
Design for modularity and scalability	Separate authentication, encryption, and webhook processing into independent, scalable components	☐	☐
Extend Zero Trust controls	Ensure Zero Trust controls can be deployed across Google, AWS, Azure, on-premises, air-gapped environments, and edge devices	☐	☐

3 | Improve Usability & Flexibility

ACTION	WHAT'S REQUIRED	NEED TO DO	DONE
Reduce complexity with API-first security	Replace complex infrastructure configurations and security appliances with simple API calls	☐	☐
Accelerate development with SDKs	Integrate encryption using native SDKs for TypeScript/JavaScript, Python, and Golang	☐	☐
Minimize operational overhead	Eliminate the need for specialized security infrastructure or extensive training with developer-friendly APIs	☐	☐
Deploy incrementally without disruption	Add zero-trust data controls to existing applications without architectural rewrites	☐	☐

4 | Implement Risk Management

ACTION	WHAT'S REQUIRED	NEED TO DO	DONE
Verify regulatory alignment	Confirm your encryption solution meets FedRAMP, CMMC, and defense computing standards	☐	☐
Enable data sanitization and classification	Develop systems to remove historical records and obscure sensitive data for complex compliance scenarios.	☐	☐
Enable dynamic policy enforcement	Adjust access policies in real-time based on threat intelligence and behavioral analytics	☐	☐
Prepare for audits with built-in logging	Maintain comprehensive records of all access requests, policy decisions, and key state changes	☐	☐

REFERENCES

1. https://www.cio.com/article/3962906/why-81-of-organizations-plan-to-adopt-zero-trust-by-2026.html
2. https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have implemented-a-zero-trust-strategy
3. https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have implemented-a-zero-trust-strategy
4. https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have implemented-a-zero-trust-strategy

qanapi

Introducing Qanapi

THE ONLY API DELIVERING ZERO TRUST AT THE DATA LAYER

Qanapi Karst_Gorge is an encryption API that binds identity, policy, and encryption as one atomic transaction at the data object. This is the control that keeps access rules attached to source code, secrets, and customer records across services, clouds, and pipelines.

This API-first approach dramatically simplifies the security burden on development teams. Instead of wrestling with complex infrastructure configurations or sprawling security appliances, developers can implement robust Zero Trust principles with minimal overhead and faster time-to-market.

Zero Trust Policy

CUSTOM POLICIES:

- Identity & Access Control
- Data Classification & Tagging
- Encryption & Key Management
- Context-Aware & Conditional Access
- Compliance & Governance
- Behavioral & Adaptive Trust

Encryption

AES-256

FIPS 140-3 and quantum resistant

Symmetric

Want to ensure your data is truly secure in 2026?

Book a demo →