QUANTUMVAULT

PQC Enterprise Security by Dytallix

TECHNICAL WHITEPAPER

PREPARING ENTERPRISE SECURITY FOR THE Y2Q DEADLINE

Executive Summary

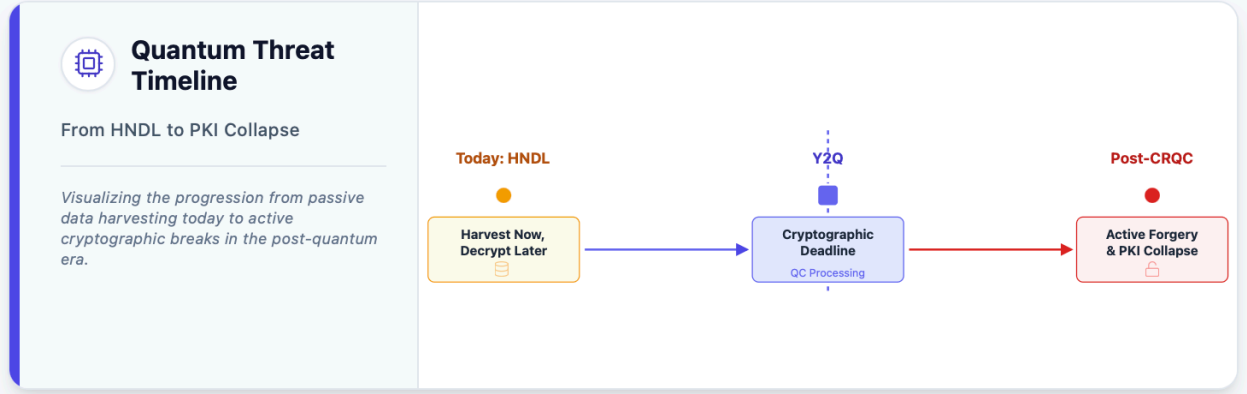
QuantumVault is a post-quantum–hardened data protection and cryptographic transition platform designed to address the full lifecycle of quantum risk.

It protects sensitive data against present-day Harvest-Now-Decrypt-Later (HNDL) collection and future cryptographically relevant quantum computer (CRQC) attack by replacing vulnerable cryptographic trust anchors with NIST-standardized post-quantum primitives and enforcing strict zero-trust and policy-driven controls.

QuantumVault is positioned for CTOs, CIOs, and CISOs responsible for long-lived data, regulated environments, and systems where cryptographic failure equates to irreversible loss, regulatory breach, or operational shutdown.

1. The Market Reality: Cryptography Has a Hard Deadline

The transition to post-quantum security is not driven by theoretical research milestones or speculative forecasts. It is driven by a structural mismatch between classical cryptographic assumptions and the capabilities of fault-tolerant quantum computers. Once that mismatch is crossed, failure is immediate and systemic. This section establishes why the timeline is fixed, why partial mitigations fail, and why delay compounds risk rather than deferring it.



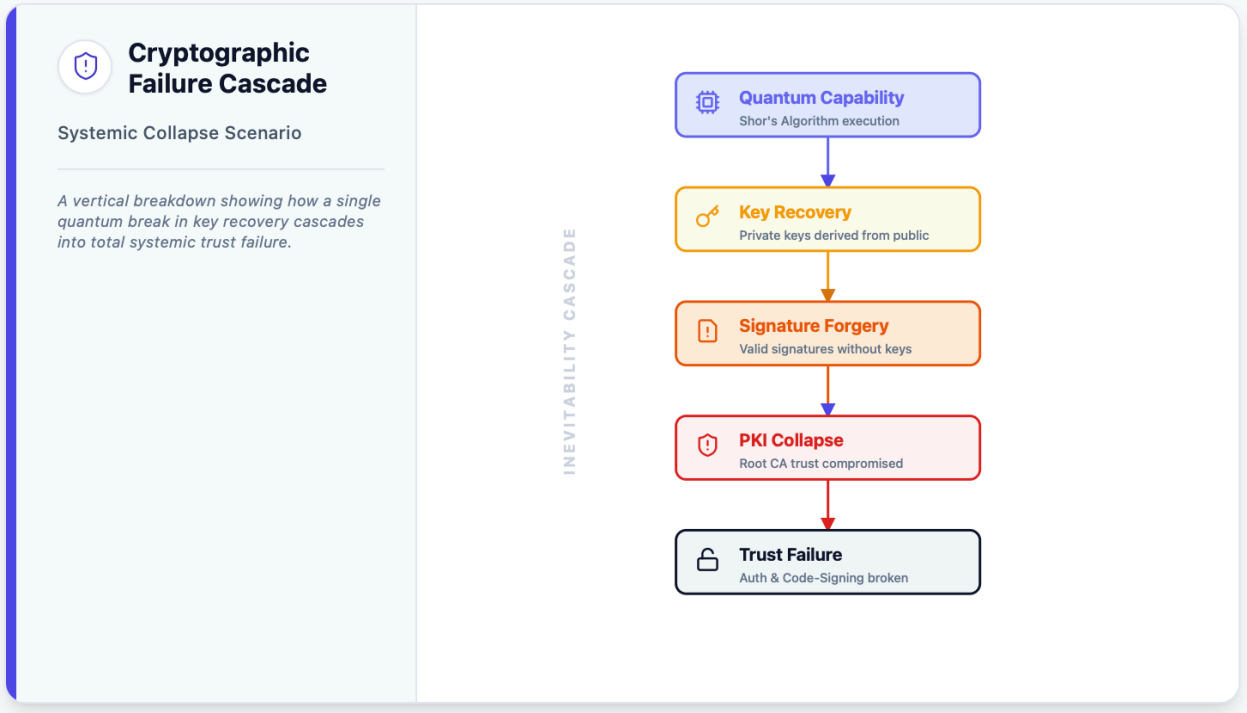
1.1 THE END OF CLASSICAL PUBLIC-KEY CRYPTOGRAPHY

RSA, Diffie–Hellman, and elliptic-curve cryptography are mathematically incompatible with fault-tolerant quantum computers.

Shor-class attacks reduce their security from infeasible to polynomial time. This is a structural failure, not a vulnerability that can be patched.

Once CRQCs reach utility scale:

- Key recovery becomes practical.
- Digital signatures become forgeable.
- PKI trust chains collapse.
- Authentication, authorization, and code-signing fail simultaneously.



1.2 HARVEST NOW, DECRYPT LATER IS ALREADY ACTIVE

Quantum adversaries are already collecting encrypted traffic and archives with the explicit intent to decrypt them later.

Any data encrypted today under classical asymmetric cryptography and required to remain confidential beyond the Y2Q horizon (≈2030–2035) should be considered compromised by default.

This creates **retroactive exposure**: today's compliance posture does not protect tomorrow's disclosures.

2. What QuantumVault Is

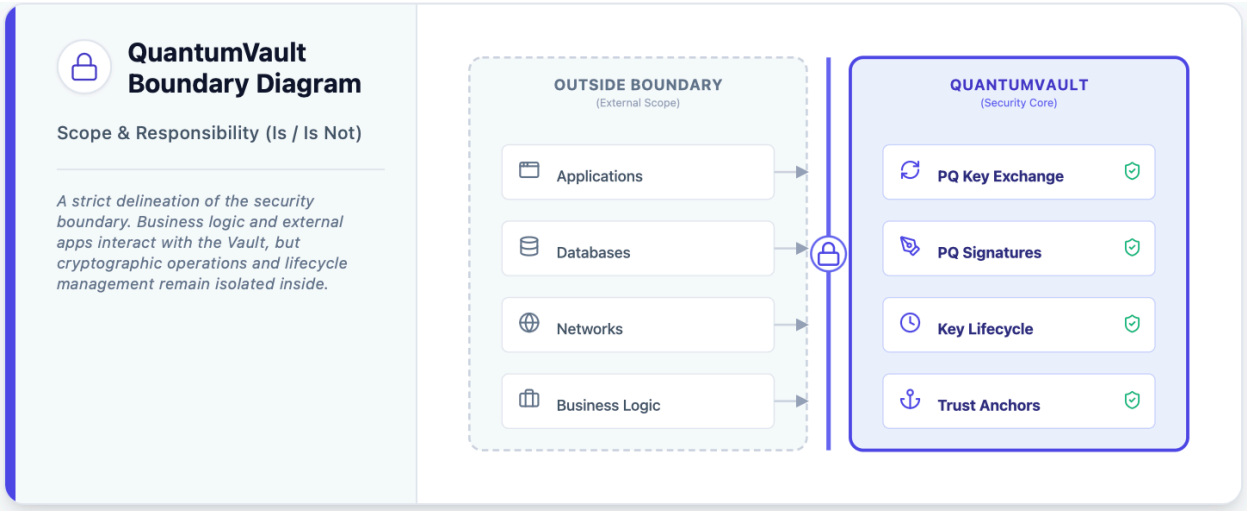
QuantumVault is a **cryptographic control plane** that enables organizations to:

- Protect data at rest and in transit using post-quantum–safe key establishment.
- Replace vulnerable asymmetric cryptography without waiting for emergency cutovers.
- Enforce policy-based key lifecycle management across tenants, regions, and regulatory domains.
- Maintain long-term confidentiality and integrity guarantees independent of quantum timelines.

QuantumVault is deployed entirely within the client's environment. It operates as a client-side control plane integrated directly into existing enterprise storage, transport, and identity systems. There is no external SaaS dependency and no off-premises custody of keys or data.

3. What QuantumVault Is Not

- It is not a classical vault with PQC wrappers.
- It is not a trustless bridge inheriting legacy cryptographic risk.
- It is not dependent on elliptic-curve or RSA fallback paths.
- It does not assume cryptographic agility can be executed safely under crisis conditions.



QuantumVault enforces a deliberate break from compromised cryptographic assumptions.

4. Architecture Overview

This section describes how QuantumVault is structured and where it integrates within an existing enterprise environment. The intent is to clarify scope, integration boundaries, and responsibility lines so that architectural impact is immediately understandable. Rather than introducing a parallel stack, QuantumVault is designed to insert post-quantum security precisely at the points where classical trust anchors currently fail.

4.1 POSITION IN THE ENTERPRISE STACK

QuantumVault is a **client-resident cryptographic control plane** that sits:

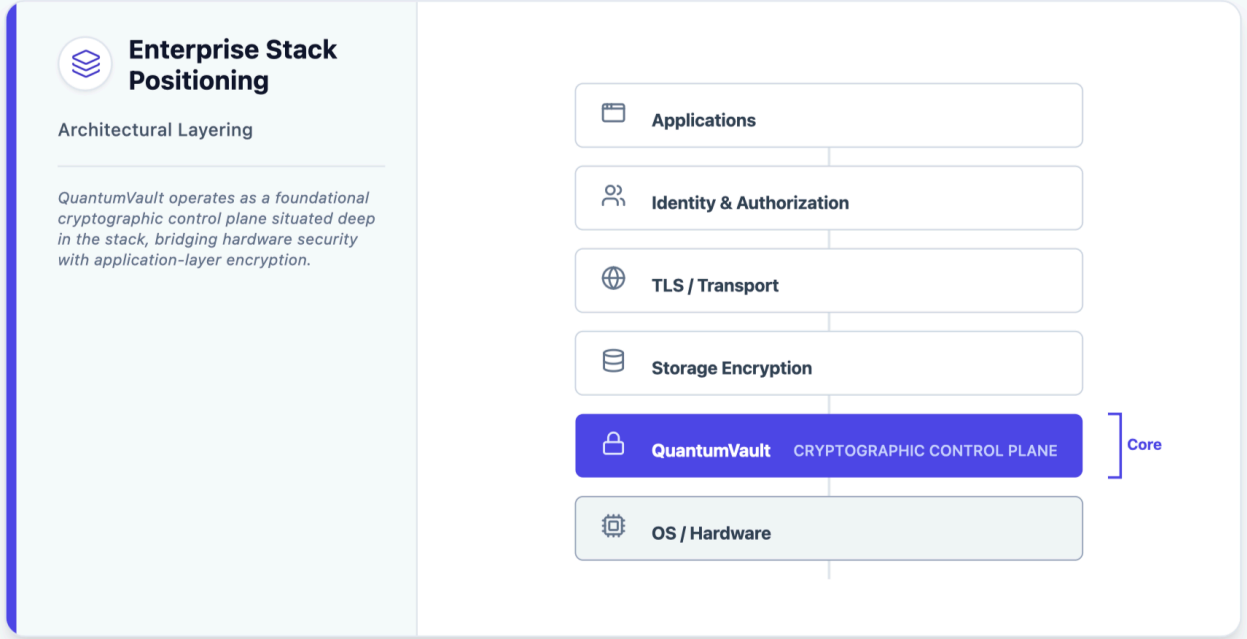
- Below applications (transparent to business logic)
- Alongside identity and key management systems (IAM, HSM, KMS)
- At TLS termination points and storage encryption boundaries

It operates **north of raw hardware** but **south of applications,** enforcing cryptographic policy at the exact layers where classical cryptography currently fails.

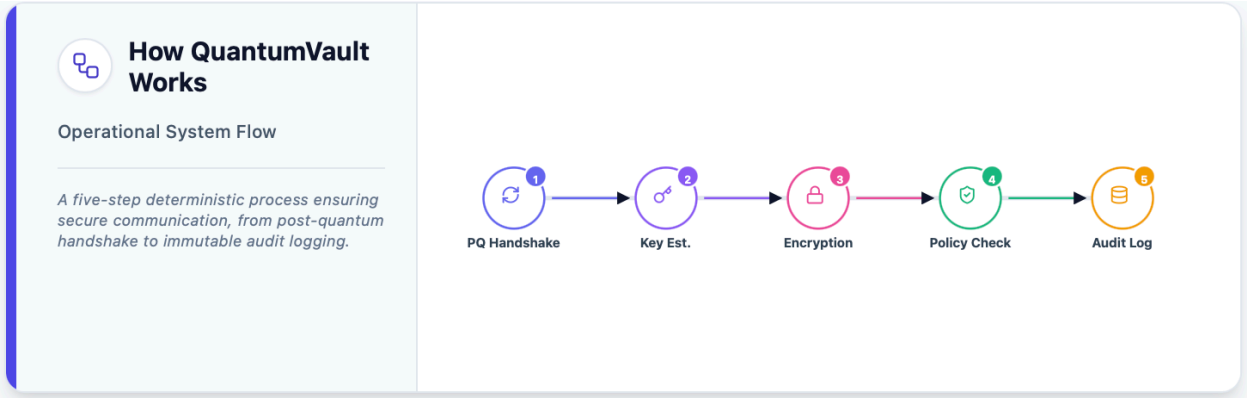
QuantumVault does **not** replace applications, databases, or networks. It replaces the **trust anchors** those systems rely on.

4.2 CORE COMPONENTS

- **PQC Key Exchange Module**: NIST-standardized KEMs for session establishment and key encapsulation.



- **PQC Signature Module**: Quantum-resistant signatures for authentication, authorization, and code integrity.
- **Encrypted Storage Engine**: Block- and object-level encryption using symmetric keys protected by PQC-wrapped key envelopes.
- **Secure Transport Layer**: PQC-hardened TLS and tunnel profiles resistant to HNDL.
- **Policy Orchestrator**: Centralized enforcement of rotation, revocation, geo-fencing, and tenant isolation.



4.3 SYSTEM FLOW

- Client initiates a post-quantum–safe handshake.
- Session keys are established using PQC KEMs.
- Data is encrypted with symmetric algorithms; keys are protected via PQC envelopes.
- Policy engine enforces lifecycle, access, and compliance constraints.

No classical asymmetric keys exist within the security boundary.

5. Security Model

This section defines the concrete security properties QuantumVault enforces and the specific failure modes it is designed to prevent. Rather than describing abstract cryptographic strength, it maps post-quantum primitives to operational guarantees: what remains confidential, what cannot be forged, and how blast radius is contained when systems fail or are compromised.

5.1 CONFIDENTIALITY

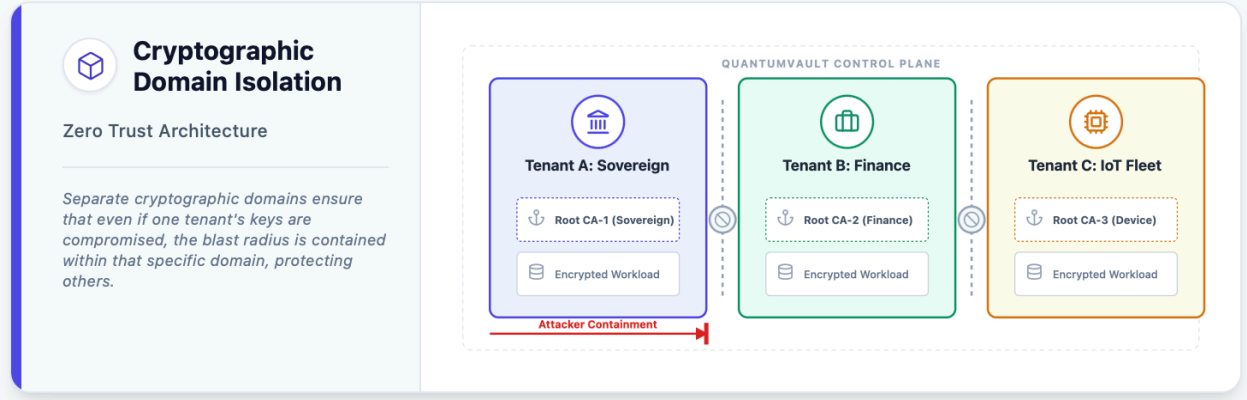
All data-in-transit and key exchange paths are resistant to HNDL collection. Recorded ciphertext cannot be decrypted retroactively.

5.2 INTEGRITY

Authorization and signing rely on post-quantum–secure schemes. Signature forgery remains computationally infeasible under known quantum models.

5.3 ISOLATION

Each tenant, system, and workload operates within a discrete cryptographic domain. Breach containment is enforced cryptographically, not procedurally.



5.4 WHY THIS IS NOT “JUST PQC TLS”

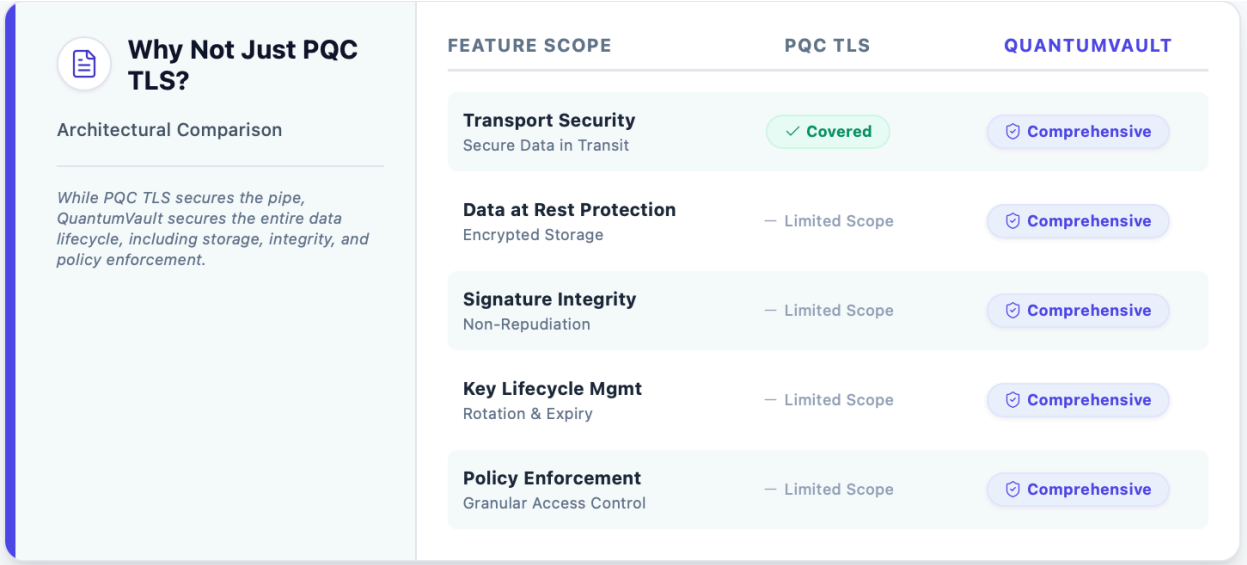
PQC-enabled TLS alone is insufficient:

- TLS protects **transport**, not data at rest.
- TLS does not address **signature forgery** for authentication, code-signing, or policy enforcement.
- TLS does not manage **key lifecycle, rotation, or revocation** across storage, identity, and applications.

QuantumVault extends post-quantum security across:

- Transport
- Storage
- Authentication and authorization
- Key lifecycle and governance

It closes the gaps left by point solutions.



6. Industry Use Cases

This section illustrates where quantum risk translates directly into material business, regulatory, and safety exposure. The industries highlighted share a common trait: the confidentiality, integrity, or authenticity of their data must survive well beyond the Y2Q horizon.

FINANCIAL SERVICES

- Long-term retention of trade, settlement, and audit records.
- PQC-hardened interbank and cross-border data exchange.
- Regulatory alignment with SEC, FINRA, PCI-DSS, PSD2.

HEALTHCARE AND LIFE SCIENCES

- Protection of PHI, genomic data, and longitudinal patient records.
- Secure inter-provider data exchange with multi-decade confidentiality requirements.
- HIPAA, HITECH, GDPR alignment.

GOVERNMENT AND DEFENSE

- Classified and sensitive-but-unclassified data protection.
- Quantum-safe inter-agency communications.
- Alignment with FedRAMP, FISMA, CMMC.

ENERGY AND CRITICAL INFRASTRUCTURE

- Secure storage of SCADA telemetry and grid control archives.
- Post-quantum authorization for operational command paths.
- NERC CIP and IEC 62443 alignment.

HIGH-TECH AND MANUFACTURING

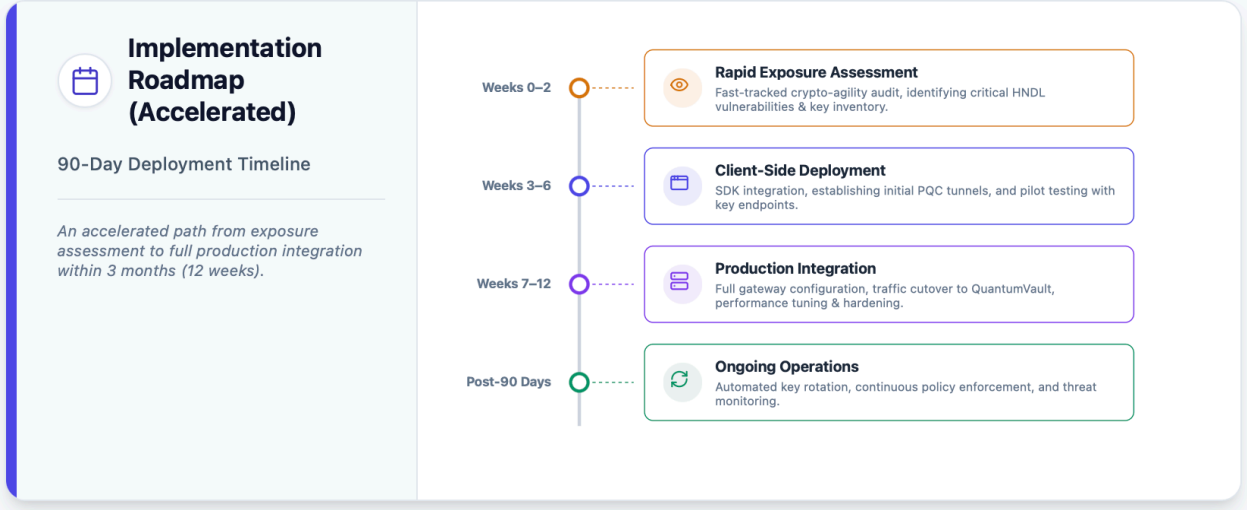
- IP protection for CAD, firmware, and R&D pipelines.
- PQC-secure code-signing for device lifecycle management.

For these sectors, post-quantum security is not an optimization.

It is a prerequisite for continuity.

7. General Implementation Timeline

This section outlines a realistic, engineering-led path for deploying QuantumVault within an existing enterprise environment.



The timeline is structured to minimize operational disruption while front-loading risk reduction, ensuring that exposure to HNDL and post-quantum failure modes is addressed early rather than deferred to later phases.

8. Compliance and Standards Alignment

QuantumVault aligns with existing regulatory and standards frameworks while addressing a core gap those frameworks implicitly assume away: the long-term viability of classical cryptography.

Rather than treating compliance as documentation layered on top of fragile controls, QuantumVault embeds compliance directly into cryptographic and policy enforcement, ensuring that regulatory guarantees remain valid across extended retention periods and future threat models.

8.1 POST-QUANTUM STANDARDS ALIGNMENT

QuantumVault is built exclusively on NIST-standardized PQC primitives:

- **NIST FIPS 203 (ML-KEM)** for quantum-resistant key establishment.
- **NIST FIPS 204 (ML-DSA)** for authentication, authorization, and integrity.
- **NIST FIPS 205 (SLH-DSA)** for long-horizon and cold-storage signing.

This anchors QuantumVault to globally recognized standards with defined security assumptions and validation pathways.

8.2 TRANSITION GUIDANCE AND VALIDATED BOUNDARIES

QuantumVault operationalizes NIST SP 800-208 transition guidance by enabling incremental, client-side deployment and early hardening of high-risk data and transport paths. Classical asymmetric cryptography is eliminated within the protected boundary rather than deferred through compensating controls.

The system is designed to integrate with **FIPS 140-3–validated** cryptographic modules, supporting explicit, auditable boundaries suitable for regulated environments and third-party review.

8.3 REGULATORY ALIGNMENT BY DESIGN

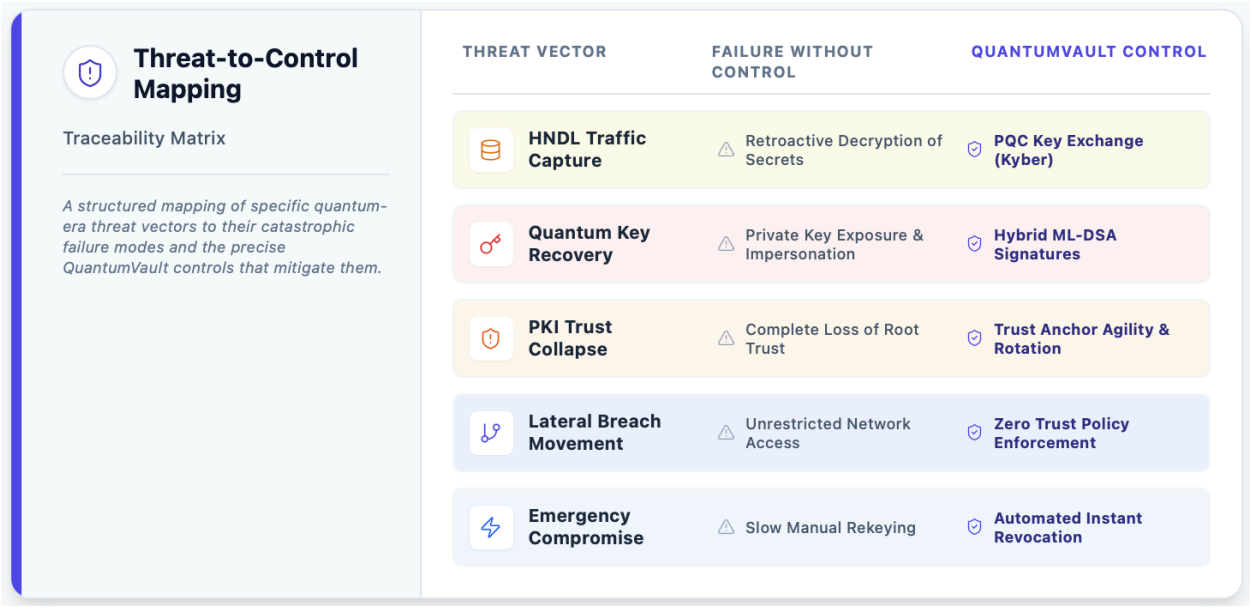
QuantumVault supports major regulatory regimes by preserving the cryptographic guarantees those regimes rely on:

- **GDPR** and privacy frameworks requiring long-term confidentiality and integrity.
- **HIPAA / HITECH** protections for extended PHI retention.
- **PCI-DSS** durability for cardholder and transaction data.

Compliance is enforced at the **cryptographic and policy layer**, reducing reliance on procedural compensating controls and minimizing compliance drift over time.

9. Threat-to-Control Mapping

This section provides a direct mapping between quantum-era threat vectors and the concrete controls QuantumVault enforces to neutralize them. The intent is to make risk reduction explicit and traceable, allowing security leaders to tie architectural decisions directly to threat mitigation and operational outcomes.



This mapping is intentionally concrete: each control corresponds to a specific failure mode that becomes unavoidable once classical cryptography collapses.

Together, they illustrate how QuantumVault converts abstract quantum risk into bounded, enforceable engineering controls rather than reactive incident response.

10. Strategic Value

QuantumVault converts quantum risk from an undefined future event into a bounded, engineered control problem.

Organizations that deploy early avoid:

- Emergency cryptographic migrations.
- Retroactive data exposure.
- Irrecoverable key compromise.
- Regulatory failure under disclosure events.

Conclusion

Quantum computing does not degrade classical cryptography.

It invalidates it.

QuantumVault provides a deployable, standards-aligned path to post-quantum security that protects data today and preserves trust tomorrow.

Assets secured under QuantumVault do not require rescue when the quantum transition arrives.