Post-Quantum Cryptography: Securing Multi-Cloud APIs Against Quantum Threats

Quantum computing advancements threaten to render traditional encryption standards obsolete. Organizations must prioritize the transition to quantum-resistant protocols to safeguard sensitive multi-cloud data.

By: Rajasingh Ramdas
Senior Technical Architect at IBM

The Threat Is Already Here

Harvest-Now, Decrypt-Later

Adversaries are **collecting encrypted API traffic today** to decrypt it once quantum computers arrive. Data with long confidentiality horizons trade secrets, health records, strategic plans is already at risk.

RSA, Diffie-Hellman, and ECC will all be broken by Shor's algorithm running on a sufficiently powerful quantum computer.

What Quantum Computers Actually Break

Broken by Quantum

RSA, ECDH, ECDSA — all public-key systems relying on integer factorization or discrete logarithms

Survives Quantum

AES, SHA-256 — symmetric encryption and hash functions require only larger key sizes (Grover's algorithm, quadratic speedup only)

The API Attack Surface

North-South Traffic

External clients to API gateways — the primary perimeter, but not the only one

East-West Traffic

Service-to-service within and across clouds — equally vulnerable to HNDL attacks

Hybrid Connectivity

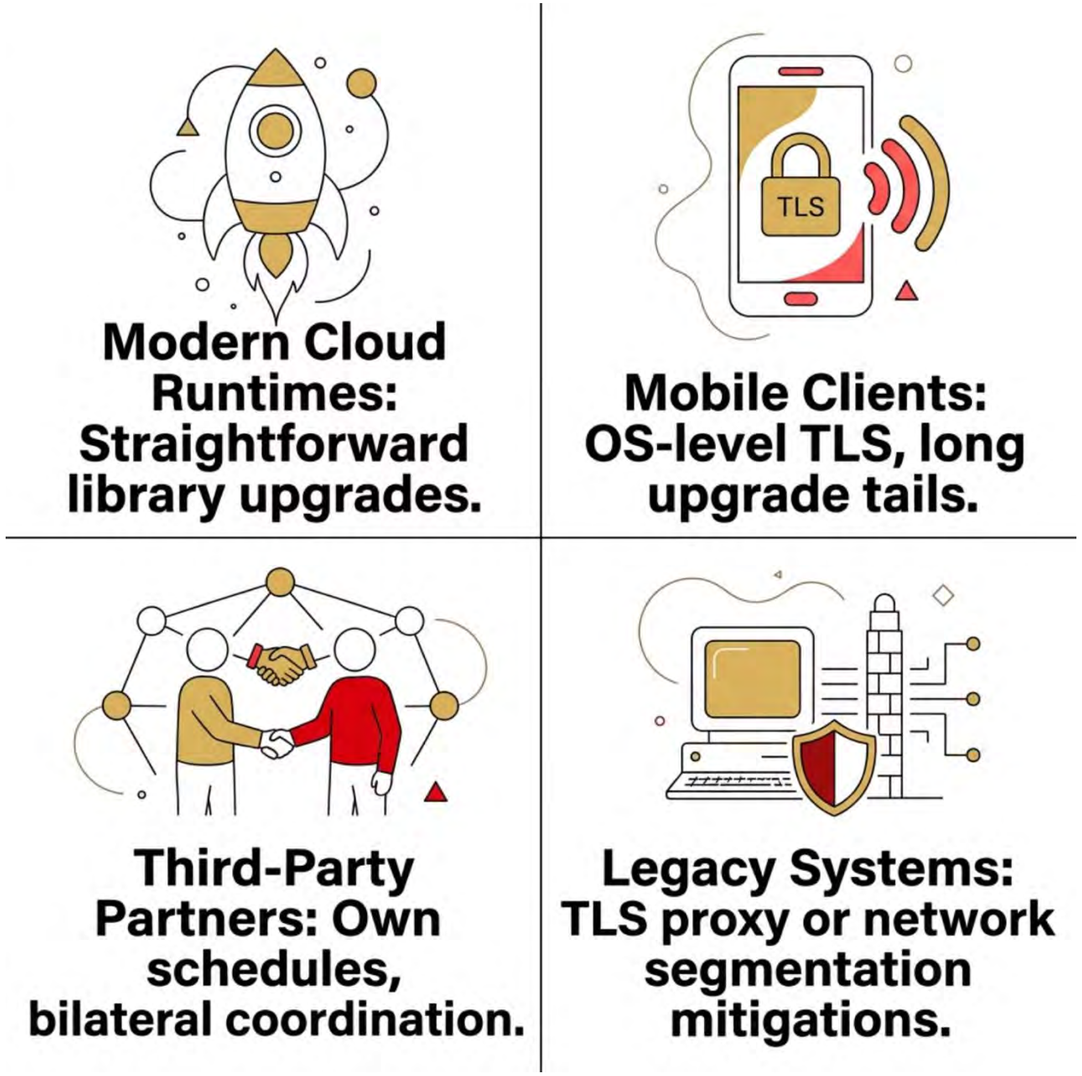
Cloud-to-on-premises links via VPN or dedicated connections

Certificate Infrastructure

Internal CAs, service mesh mTLS, and all certificate management tooling must also migrate

A quantum-resistant outer perimeter is insufficient if internal east-west communications remain classically secured.

Multi-Cloud Complexity



No Single Migration Path

Different cloud platforms have different TLS implementations, support timelines, and tooling ecosystems. Legacy components that cannot be upgraded require **network segmentation or TLS termination proxies** rather than direct cryptographic upgrades.

Risk Assessment Framework

Building a comprehensive cryptographic asset inventory is the essential first step — and typically reveals surprises in large enterprise environments.

Three Dimensions of Risk Priority

1

Data Confidentiality Lifetime

Data that must stay secret for **decades** carries far higher HNDL risk than data worthless within days

2

API Criticality

Revenue impact, regulatory scope, data sensitivity, and exposure to high-threat actors

3

Migration Feasibility

Distinguish near-term actionable items from longer-horizon items requiring vendor coordination or architectural redesign

NIST Post-Quantum Standards

The multi-year standardization process is officially complete, marking a pivotal shift in the global cryptographic landscape. Organizations can now build against **stable, published specifications**, finally removing the historical blocker of algorithm uncertainty that has slowed industry adoption.

With these standards finalized, the era of "wait and see" has ended. Enterprise leaders must now prioritize transition roadmaps, as algorithm uncertainty is no longer a valid justification for delaying critical **post-quantum readiness**.

The NIST PQC Portfolio

ML-KEM (Kyber)

FIPS 203 — Replaces RSA/ECDH for key encapsulation in TLS. Fast performance; larger keys and ciphertexts than ECC.

ML-DSA (Dilithium)

FIPS 204 — Replaces RSA/ECDSA for digital signatures. Good signing speed; significantly larger signatures than ECDSA.

SLH-DSA (SPHINCS+)

FIPS 205 — Hash-based signatures. Slower signing, very large signatures, but security rests on hash functions alone — valuable diversity of assumptions.

FN-DSA (FALCON)

FIPS 206 (forthcoming) — Lattice-based signatures with compact size, complementing the portfolio.

All lattice-based algorithms have withstood extensive public cryptanalysis during the NIST process. Confidence is substantial — though lattice cryptography has a shorter track record than RSA or ECC.

Hybrid Cryptography: Defense-in-Depth

Why Hybrid?

Run a **classical algorithm and a post-quantum algorithm in parallel**. An attacker must break both to compromise the session.

- If PQC has an unexpected flaw, classical provides the backstop
- If classical is broken by quantum, PQC provides protection
- Standardized for TLS: combine ECDH + ML-KEM, derive session key from both

Hybrid is the recommended deployment strategy — not a wholesale replacement of classical algorithms.

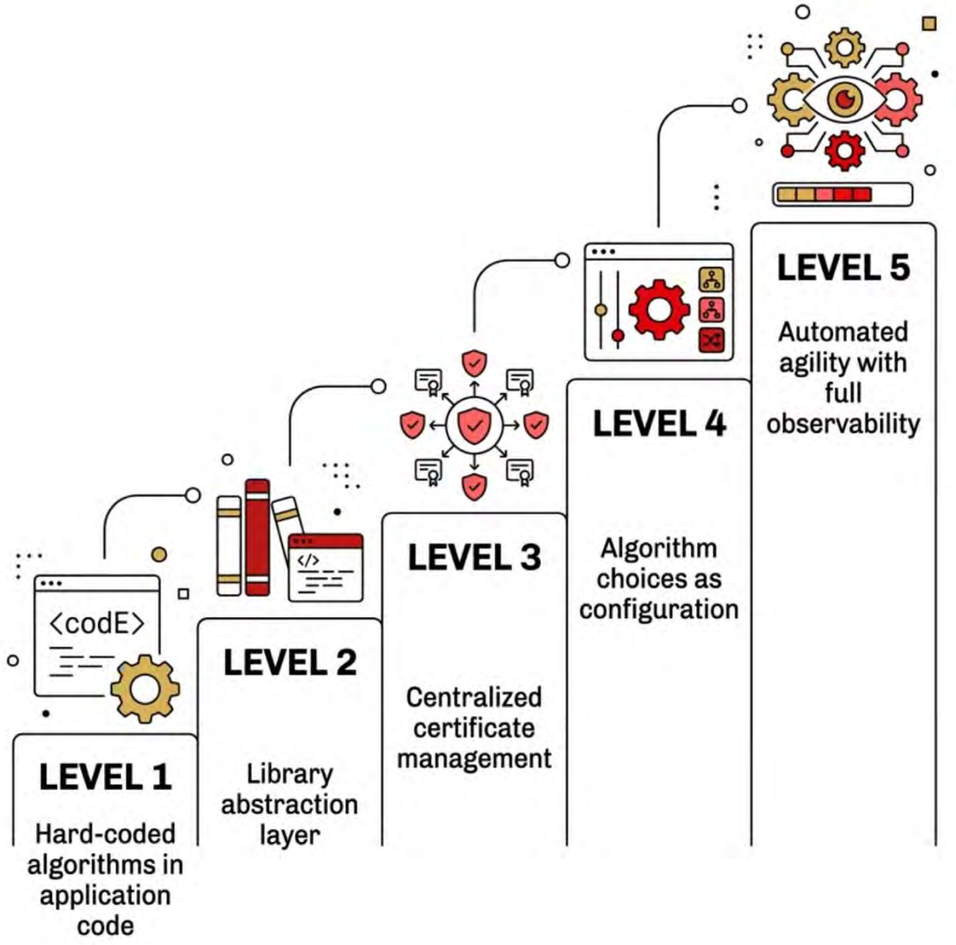
Cryptographic Agility

Design for Change

Cryptographic agility — the ability to update algorithms without fundamental architectural changes — is the force multiplier for this migration and every future one.

- Algorithm choices as configuration, not hard-coded assumptions
- Automated, centralized certificate management
- Cryptographic libraries abstracted behind stable interfaces

Systems with strong agility will be **dramatically easier to migrate** than those with cryptographic choices baked into application code.



Performance: The Real Costs

Larger Keys & Ciphertexts

ML-KEM and ML-DSA produce significantly more bytes on the wire than ECC — directly increasing TLS handshake size, latency on high-latency networks, and gateway compute cost

Compute Overhead

ML-KEM operations are fast and comparable to ECDH. ML-DSA signing is more expensive than ECDSA. Hardware acceleration is in early stages but will mature with adoption.

Mitigation Strategies

Session resumption, connection pooling, HTTP/2 and HTTP/3 multiplexing, and tiered deployment (high-risk traffic first) all reduce the practical performance impact

Benchmark in your actual environment. Research paper numbers do not capture production load patterns, connection durations, or hardware configurations.

Migration Roadmap

1

Phase 1: Foundation

Cryptographic asset inventory, risk framework, library selection, vendor engagement, performance testing in non-production

2

Phase 2: High Priority

Hybrid TLS on external API gateways for high-sensitivity data; service mesh migration for critical east-west traffic; internal CA migration

3

Phase 3: Broad Rollout

Lower-priority APIs, partner integrations, externally issued certificate chain migration

4

Phase 4: Hard Cases

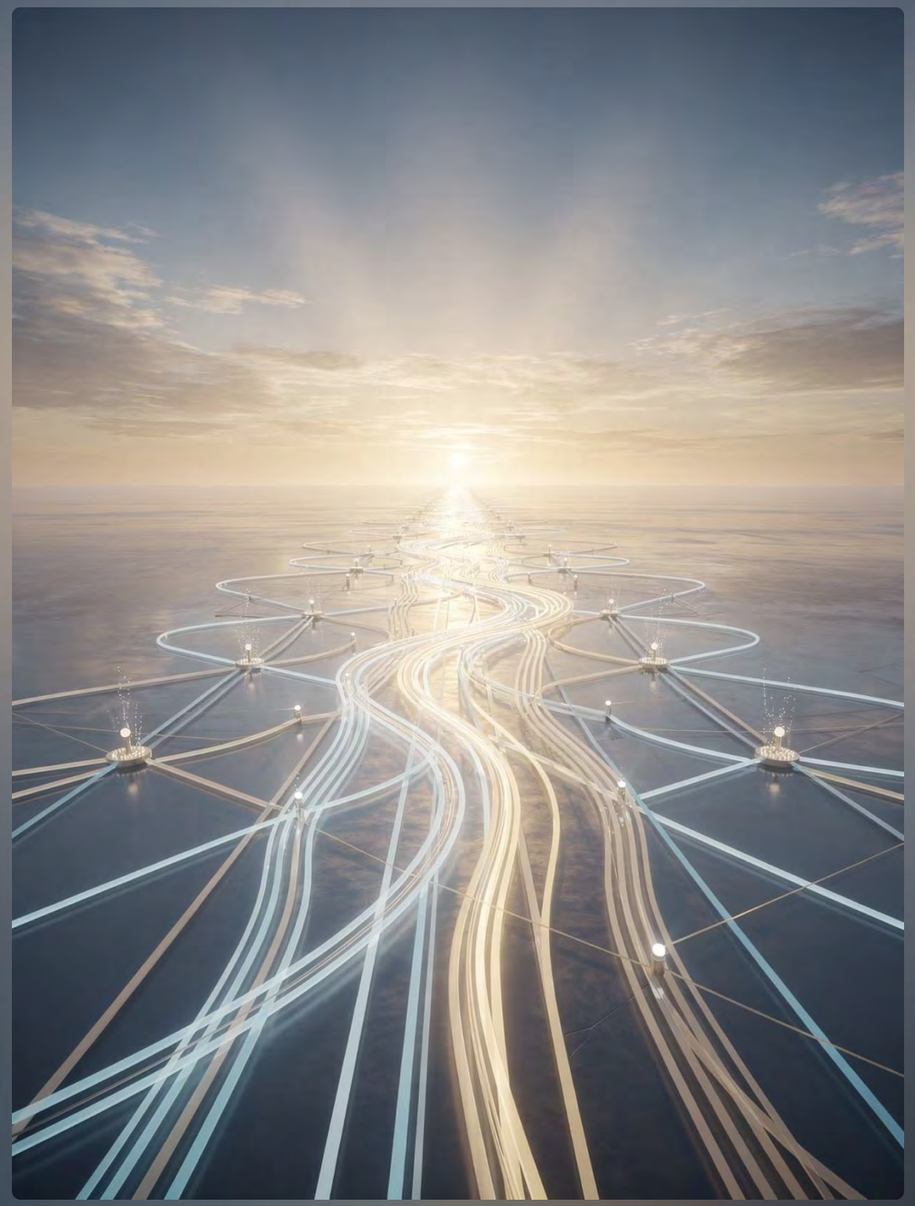
Legacy architectural mitigations, long-tail client compliance, ongoing cryptographic agility maintenance

Organizational Dynamics

This Is a Program, Not a Project

Post-quantum migration touches **networking, security, platform engineering, application development, partner management, and procurement**. It requires sustained executive sponsorship over a multi-year timeline.

- Frame in business terms: risk reduction, regulatory compliance, customer trust
- Regular governance reviews of threat, standards, and vendor support landscapes
- Uncertainty about quantum timelines is **not** a justification for inaction



The Time to Begin Is Now

HNDL Is Present-Day

Data transmitted today may already be archived for future quantum decryption

Standards Are Ready

NIST FIPS 203–205 are published and stable. Library support is maturing rapidly.

Migration Takes Years

Organizations beginning today will still be working through long-tail cases when the threat is concretely visible

Collateral Benefits

The cryptographic hygiene work uncovers misconfigurations and weak cipher suites that strengthen security *immediately*

> The quantum threat to APIs is real, the tools to address it are available, and the time to begin is now.

Thank You