

POST-QUANTUM CRYPTO MIGRATION.

A quantum computer capable of breaking today's public-key cryptography doesn't exist yet — **but adversaries are already harvesting encrypted traffic to decrypt the moment one does**, which is why migration has to start now.

- HARVEST NOW, DECRYPT LATER
- NIST PQC STANDARDS (FIPS 203-205)
- HYBRID CRYPTOGRAPHY
- CRYPTOGRAPHIC AGILITY

01 THE MECHANISM



Harvest Now, Decrypt Later

Adversaries are already recording today's encrypted traffic, betting a future quantum computer will let them decrypt it retroactively — **data that must stay confidential for years is already exposed** to a threat that doesn't exist yet.



Shor's Algorithm Breaks Public-Key Math, Not Symmetric Keys

A sufficiently powerful quantum computer efficiently solves the factoring and discrete-log problems behind RSA, Diffie-Hellman, and ECC — **but only weakens AES by a quadratic factor**, so symmetric encryption needs a bigger key, not a new algorithm.



Cryptographic Agility Over a Single Algorithm Bet

NIST's own SIKE candidate was broken by a classical computer after years of scrutiny — **the ability to swap algorithms without redesigning the whole system matters more** than trusting any one scheme permanently.

02 THE FLOW

The Crypto-Agile Migration

CONTAINED

1

A cryptographic inventory identifies every certificate, protocol, and embedded system using vulnerable public-key algorithms, including long-lived firmware signing roots.

2

Hybrid key exchange combines a classical algorithm with ML-KEM in the same handshake, so **security holds as long as either scheme remains unbroken** during the transition.

3

Systems are built with swappable cryptographic modules, so **a future weakness in one PQC algorithm means an update, not a redesign**.

The Single-Algorithm Bet

EXPOSED

1

No cryptographic inventory exists, so vulnerable RSA and ECC usage in legacy systems and long-lived firmware goes undiscovered until it's urgent.

2

A single new algorithm is hardcoded everywhere at once with no classical fallback, so **a future break in that one scheme leaves nothing to fall back on**.

3

Confidential data encrypted today with classical-only algorithms is **already being harvested** by adversaries betting on tomorrow's quantum decryption.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Cryptographic Inventory & Discovery	Identifies every system, certificate, protocol, and embedded device using vulnerable public-key cryptography, including dependencies most organizations haven't already mapped.
NIST-Standardized PQC Algorithms	Adopts ML-KEM for key establishment and ML-DSA or SLH-DSA for signatures, the finalized FIPS 203/204/205 standards published in 2024.
Hybrid Cryptography During Transition	Combines a classical algorithm with a PQC algorithm in the same operation, so security holds even if one scheme is later broken.
Cryptographic Agility	Designs systems to swap algorithms without a full redesign, since PQC standards themselves may still evolve as cryptanalysis continues.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Wait Until a Quantum Computer Actually Exists	No	Ignores harvest-now-decrypt-later; data encrypted today with classical algorithms is already being collected for future decryption.
Migrate Signatures Only, Skip Key Exchange	No	Leaves confidentiality exposed to harvesting even if authenticity is addressed, missing half the actual threat.
Adopt a Single New PQC Algorithm With No Fallback	No	Repeats the exact risk that broke SIKE, a single scheme with no hybrid fallback if cryptanalysis finds a weakness.
Assume Symmetric Encryption (AES) Needs Replacing Too	No	Misdirects migration effort; AES only needs a larger key size, not a new algorithm, unlike RSA/ECC which need full replacement.
Full Inventory + NIST-Standardized Algorithms + Hybrid Transition + Cryptographic Agility	Yes	Addresses discovery, algorithm choice, transition risk, and future flexibility together, rather than solving only one piece.

POST-QUANTUM CRYPTO MIGRATION.

ASSESS · MIGRATE · VERIFY

05 PROGRAM OPERATIONS

The urgency is about data lifespan, not quantum computer timelines. Anything that must stay confidential longer than it takes a quantum computer to arrive is already at risk today.

Long-lived signed artifacts need PQC even sooner than encrypted traffic. Firmware and root certificates signed today may need to stay trustworthy for a decade, making re-signing after the fact impractical.

NIST's own selection process shows why agility matters. SIKE was a round-4 candidate broken by a classical attack in 2022, after years of public cryptanalysis found nothing wrong with it.

Larger keys and signatures aren't a footnote. ML-KEM and ML-DSA both produce meaningfully larger key and signature sizes than their classical counterparts, straining bandwidth-limited or embedded systems.

06 CONTROL MAPPING

NIST FIPS 203 (ML-KEM)

The standardized key-encapsulation mechanism, based on CRYSTALS-Kyber, for general-purpose public-key encryption and key establishment.

NIST FIPS 204 / 205 (ML-DSA / SLH-DSA)

The standardized digital signature algorithms, based on CRYSTALS-Dilithium and SPHINCS+ respectively, offering different underlying mathematical assumptions.

NATIONAL SECURITY MEMORANDUM 10 (NSM-10)

The 2022 U.S. directive requiring federal agencies to inventory cryptography and prioritize migration to quantum-resistant algorithms.

CNSA 2.0

NSA's Commercial National Security Algorithm Suite 2.0, setting specific PQC transition timelines for National Security Systems.

07 WHAT THIS DOES NOT SOLVE

Legacy & Embedded System Replacement

Standardizing an algorithm doesn't retrofit it into hardware and firmware never designed to be updated, a major share of the real-world migration effort.

Post-Quantum Threats to Symmetric Crypto

PQC migration targets public-key algorithms; it doesn't change the separate, much smaller adjustment symmetric encryption and hashing need.

Algorithm Stability Guarantees

NIST standardization reflects the best current cryptanalysis, not a permanent guarantee — continued research could still surface weaknesses, which is exactly why agility matters.

Non-Cryptographic Quantum Risk

Migrating algorithms doesn't address other potential quantum-era risks to authentication, randomness generation, or protocol design that aren't purely about the crypto primitive.

08 MYTHS VS. REALITY

MYTH "Post-quantum cryptography migration can wait until quantum computers actually exist."	REALITY Harvest-now-decrypt-later means adversaries are already collecting today's encrypted traffic to decrypt once a capable quantum computer arrives — the data is exposed now, not later.
MYTH "AES and other symmetric encryption need to be replaced too."	REALITY Quantum computers only give a quadratic speedup against symmetric algorithms via Grover's algorithm — doubling the key size restores the security margin, no new algorithm required.
MYTH "Once NIST picks an algorithm, it's safe to standardize on that alone."	REALITY SIKE was a NIST round-4 finalist broken by a classical computer in 2022 after years of scrutiny — hybrid approaches and cryptographic agility exist precisely because standardization isn't a permanent guarantee.
MYTH "PQC migration is mainly a software update."	REALITY Embedded devices, firmware signing roots, and hardware with 10+ year lifespans often can't be simply patched, making inventory and long-lead-time planning as important as the algorithm choice itself.
MYTH "Hybrid cryptography is just a temporary inefficiency to tolerate."	REALITY It's a deliberate risk-mitigation strategy — combining classical and post-quantum algorithms means a break in either one alone doesn't compromise the system.

09 SPEAK THE PROGRAM — KEY TERMS

HARVEST NOW, DECRYPT LATER (HNDL)

The strategy of recording encrypted traffic today to decrypt once a cryptographically relevant quantum computer becomes available.

CRYPTOGRAPHICALLY RELEVANT QUANTUM COMPUTER (CRQC)

A quantum computer powerful enough to actually break current public-key algorithms via Shor's algorithm, not yet believed to exist.

ML-KEM (FIPS 203)

The NIST-standardized lattice-based key-encapsulation mechanism, based on CRYSTALS-Kyber, replacing classical key exchange.

CRYPTOGRAPHIC AGILITY

The ability to swap cryptographic algorithms without a full system redesign, critical given that PQC standards may still evolve.

HYBRID CRYPTOGRAPHY

Combining a classical and a post-quantum algorithm in the same operation so security holds if either one alone is broken.

SHOR'S ALGORITHM

The quantum algorithm that efficiently solves the factoring and discrete-logarithm problems underlying RSA, Diffie-Hellman, and elliptic-curve cryptography.