Quantum Readiness

Secure your Future Today

Post-Quantum Cryptography (PQC) is the **mandatory and urgent global initiative** to replace the public-key algorithms (like RSA/ECC) that a powerful quantum computer (CRQC) will break. This isn't a future problem; the **"Harvest Now, Decrypt Later"** threat means sensitive, long-term data is already at risk. With migration estimated to take 5-10 years, organizations **must start their PQC transition immediately** by inventorying assets and adopting a hybrid, crypto-agile strategy to safeguard the digital infrastructure and maintain long-term data confidentiality against the impending quantum threat.

Key Benefits
Why Transition to PQC Now?

Enduring Data Confidentiality
Protects long-term sensitive data, such as financial records, government secrets, and healthcare data, from the **"Harvest Now, Decrypt Later" (HNDL)** attack. Adversaries are storing encrypted data now, awaiting a quantum computer to decrypt it later. PQC algorithms ensure this historical and future data remains confidential for its required security lifetime.

Preserve Digital Trust
Prevents the widespread **forgery of digital signatures**, which could cripple global infrastructure. A quantum attack could undermine Public Key Infrastructure (PKI), software updates, and financial transactions. PQC-enabled digital signatures maintain the integrity of identity and authentication across all digital systems.

Secure Critical Infrastructure
Safeguards the core protocols of the internet and global commerce, including **TLS/SSL (HTTPS), SSH, and VPNs**. PQC ensures secure communications and key establishment against both classical and quantum attacks, preventing a breakdown of trust and security across the digital world.

Why Post-Quantum Cryptography (PQC) Matters Now

The foundation of modern digital security - from securing internet commerce to protecting national secrets - rests on the strength of public-key cryptography. However, this foundation is built on mathematical problems that a future, powerful quantum computer can solve in minutes, not millennia. **Post-Quantum Cryptography (PQC)** is the urgent, global effort to develop new algorithms to replace this vulnerable foundation, making digital systems resistant to this impending quantum threat. This is not a distant, theoretical concern; the window for a secure migration is closing, making PQC the defining cybersecurity challenge of the next decade.

The Existential Threat and Its Impact

The Vulnerability of Current Cryptography

Modern security relies almost exclusively on asymmetric (public-key) cryptography, primarily **RSA** and **Elliptic Curve Cryptography (ECC)**. Their security is based on mathematical problems - integer factorization and discrete logarithms, respectively - that are intractable for today's classical computers.

In 1994, mathematician Peter Shor introduced the **Shor's algorithm**, a quantum algorithm capable of solving both of these problems exponentially faster than any classical computer. A cryptographically relevant quantum computer (CRQC) - one with thousands of stable logical qubits - could break the most common encryption standards (like RSA-2048) in hours or even minutes. While a CRQC isn't here yet, its arrival is projected by many experts, including the U.S. National Institute of Standards and Technology (NIST), to be potentially within the next **5 to 15 years**.

The "Harvest Now, Decrypt Later" Threat

The most immediate and critical vulnerability is the **"Harvest Now, Decrypt Later" (HNDL)** attack. Adversaries, particularly nation-states, are already intercepting and storing vast amounts of encrypted sensitive data today, knowing that when a CRQC becomes available, they will be able to decrypt this historical traffic at will.

Regulatory Compliance
Aligns organizations with emerging **government mandates and global standards**, notably those set by NIST, CISA, and international bodies. Early migration to PQC-compliant systems helps meet deadlines for critical infrastructure and government contracts, avoiding future procurement or compliance penalties.

Achieve Crypto-Agility
Establishes the technical and operational flexibility to **rapidly switch cryptographic algorithms** without major overhauls. This resilience ensures protection against future breakthroughs in quantum computing or the potential cryptanalysis of current PQC candidates, guaranteeing long-term security.

This HNDL threat targets data with long-term confidentiality requirements, including:

- **Financial Records:** Banking and investment transactions.
- **Government & Military Secrets:** Diplomatic cables, intelligence communications, and defense technologies.
- **Healthcare Data:** Decades of patient histories and genetic research.
- **Intellectual Property (IP):** Corporate blueprints, trade secrets, and R&D data.

The time it takes to develop a CRQC is the **Threat Timeline (T_T)**. The time it takes an organization to replace all vulnerable cryptography is the **Migration Time (T_M)**. The time for which the data must remain confidential is the **Security Lifetime (T_L)**.

If *$T_T < T_L - T_M$*, the data is fundamentally at risk.

Since T_M is estimated to be 5-10 years for large organizations, the time to begin PQC migration is **now**.

Impact on Global Infrastructure

The fallout from a successful quantum attack goes beyond data breaches. It would cripple the core infrastructure of the digital world:

- **Loss of Trust:** Attackers could forge digital signatures, undermining software updates, financial transactions, and Public Key Infrastructure (PKI). This would destroy trust in digital identity and authentication.
- **Insecure Communications:** All secure internet protocols, including **TLS/SSL (HTTPS)**, **SSH**, and **VPNs**, which use RSA/ECC for key establishment and authentication, would instantly become insecure.
- **Cryptocurrency:** Blockchains and cryptocurrencies relying on ECC signatures could be vulnerable to theft, enabling an attacker to generate a legitimate signature to spend another user's funds.

Key Features
How to Achieve PQC Security

NIST Standardization
Based on the rigorous, **multi-year global competition** and selection process led by the U.S. National Institute of Standards and Technology (NIST). This ensures that selected algorithms like CRYSTALS-Kyber (ML-KEM) and CRYSTALS-Dilithium (ML-DSA) are globally vetted, secure, and ready for industry adoption as new FIPS standards.

Lattice-Based Cryptography
Utilizes mathematical problems that are thought to be **intractable even for a powerful quantum computer**. This principle forms the basis for the primary key-establishment (Kyber) and digital signature (Dilithium) algorithms, offering high security with efficient performance and small key/ciphertext sizes.

Hybrid Migration Strategy
Enables a smooth, phased transition by **simultaneously using both classical and PQC algorithms** (e.g., ECC + ML-KEM). This hybrid mode ensures immediate quantum security while maintaining backward compatibility and mitigating the risk of relying solely on an unproven PQC standard during the transition phase.

Phased Migration Roadmap
Involves a structured, long-term approach - Discovery, Pilot/Hybrid Deployment, and Full Migration. This strategic plan, endorsed by agencies like CISA, prevents a rushed, one-time fix and ensures that PQC is integrated methodically, focusing on high-priority systems first.

Global Efforts to Mitigate the Threat

NIST's Standardization Process

Recognizing the danger, the U.S. **National Institute of Standards and Technology (NIST)** initiated a global, multi-year competition in 2016 to solicit, evaluate, and standardize new quantum-resistant algorithms. This rigorous, open process has been the primary driver of PQC development worldwide.

Selected PQC Algorithms (First Set)

In 2022 and 2024, NIST announced the selection of the first set of algorithms, which are now being published as Federal Information Processing Standards (FIPS):

Standard	Algorithm Name (PQC Technique)	Purpose	Description
BIPS 203 (ML-KEM)	CRYSTALS-Kyber (Lattice-based)	Key Encapsulation Mechanism (KEM)	Designed for general encryption and key exchange (to replace Diffie-Hellman/ECC). It offers small ciphertexts and fast performance.
FIPS 204 (ML-DSA)	CRYSTALS-Dilithium (Lattice-based)	Digital Signatures (DSA)	Designed for digital authentication (to replace RSA/ECDSA). It offers high-security levels with reasonable key sizes.
FIPS 205 (SLH-DSA)	SPHINCS^{+} (Stateless Hash)	Digital Signatures (DSA)	A hash-based signature scheme providing a different mathematical foundation than lattices, serving as a secure backup option.

New Cryptographic Principles

These selected algorithms rely on mathematical problems that are thought to be difficult even for a CRQC:

- **Lattice-Based Cryptography:** Relies on the difficulty of finding the shortest vector in a high-dimensional lattice. This class of problems forms the basis for Kyber and Dilithium.
- **Hash-Based Cryptography:** Relies on the security of cryptographic hash functions (like SHA-256), which are only weakly impacted by quantum computers (Grover's algorithm halves the effective security length).

Cryptographic Asset Discovery
Requires the foundational first step of creating a **Cryptographic Bill of Materials (CBOM)**. Automated scanning tools inventory every key, certificate, and algorithm in use across the network. This visibility is essential for prioritizing the replacement of vulnerable systems with long-term confidentiality needs.

Guidance and Strategic Migration

A successful transition to PQC requires a long-term, crypto-agile strategy, not a rushed, one-time fix. Government agencies worldwide, notably the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the UK's National Cyber Security Centre (NCSC), and the Canadian Centre for Cyber Security, have established clear roadmaps.

The PQC Migration Roadmap

Organizations must follow a phased approach, broken down into manageable, strategic steps:

Phase 1: Discovery and Inventory (The Foundation)

The first critical step is gaining **full cryptographic visibility**.

- **Cryptographic Asset Discovery:** Use automated tools to scan the entire network, applications, source code, and data archives. The goal is to build a **Cryptographic Bill of Materials (CBOM)** - a comprehensive inventory of every key, certificate, and algorithm in use.
- **Prioritization:** Map assets to business criticality and data sensitivity. Identify the high-priority systems that handle long-term data secrets or critical authentication functions (e.g., firmware signing, root CAs, archived financial data).

Phase 2: Pilot and Hybrid Deployment (The Transition)

This phase introduces the new PQC algorithms without fully committing to them.

Crypto-Agility: Establish the ability to switch cryptographic algorithms easily. This often requires updating software libraries and hardware (e.g., HSMs).
Hybrid Mode: Implement **hybrid cryptography** on high-priority systems. A hybrid scheme uses **both** a classical algorithm (like ECC) and a PQC algorithm (like ML-KEM) simultaneously to establish a shared secret. This ensures that the communication is secure against both classical and quantum attacks, guaranteeing backward compatibility while mitigating the risk of future quantum decryption.

{Hybrid Key Agreement} = {Classic Key (ECC/RSA)} + {PQC Key (ML-KEM)}

Test Environment: Rigorously test PQC implementations for performance overhead, key size impact, and compatibility in a non-production environment.

Phase 3: Full Migration (The Deadline)

Based on government guidance, the deadline for full PQC migration is becoming clearer.

Government Mandates: The U.S. National Security System (NSS) roadmap targets a transition to quantum-resistant algorithms by **2035**. Other agencies are pushing for high-priority systems to be migrated by **2030-2031**. These deadlines serve as an effective mandate for the private sector, particularly critical infrastructure.

Procurement Policy: Organizations must update all procurement policies to mandate PQC-compliant products from vendors. Anything new purchased today must be quantum-safe to avoid creating new legacy debt.

Retirement: Decommission systems that cannot support PQC or replace vulnerable cryptographic modules entirely.

Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH Elliptic Curve Cryptography	Public key	Signatures, key exchange	No longer secure
DSA Finite Field Cryptography	Public key	Signatures, key exchange	No longer secure

Industry Response and Next Steps

The transition to PQC represents a global IT re-tooling effort unprecedented since the shift to the internet itself.

Key Industry Drivers

- **Cloud Providers:** AWS, Google Cloud, and Microsoft Azure are integrating PQC algorithms (like Kyber/ML-KEM) into their core services, particularly for internal and client-facing TLS connections, leading the industry adoption curve.
- **Hardware Security Modules (HSMs):** HSM vendors are rapidly releasing products with firmware capable of generating and protecting PQC keys, a critical step since HSMs serve as the root of trust for most large-scale PKI deployments.
- **PKI/Certificate Management:** Tools are emerging to handle the new complexity of managing millions of hybrid and PQC-only certificates, including support for larger key and certificate sizes.

The Role of Crypto-Agility

Ultimately, PQC is not about selecting one final algorithm; it is about establishing **crypto-agility**. Given the potential for future breakthroughs in quantum computing or cryptanalysis of current PQC candidates, organizations must have the operational and technical flexibility to switch out cryptographic algorithms rapidly without massive infrastructure overhauls. This ensures long-term resilience against unknown threats.

In conclusion, Post-Quantum Cryptography is more than just a security upgrade; it is a **mandatory global transition** to safeguard the digital future. The quantum threat is certain, and the time required for secure migration is long. By prioritizing cryptographic discovery, embracing hybrid strategies, and adhering to the emerging global standards, organizations can move from a state of critical vulnerability to one of enduring quantum resilience. The time to act is definitively now.