

Preparing For The Post-Quantum Revolution

Colonel (Ret) Joseph Wingo

Director of Strategy, Armis Federal from ServiceNow

Post-Quantum...Yesterday's Problem

...If the “Quantum Dawn” is estimated for 2029 at the earliest, why is this “yesterday’s problem”?

1. 3-5 years from “Requirement” to “Implementation”

- Heavy lift...especially for legacy mission networks
- Poor situational awareness of current cryptographic utilization

2. “Harvest Now...Decrypt Later” tactics

- Extrapolations based on old planning data
- Requirements for development of future weapon systems
- Analysis of user user/system behavior
- Every year of delay = more vulnerable traffic in adversary hands

Post-Quantum...Yesterday's Problem

3. Regulatory requirements

- NIST phasing out quantum-vulnerable algorithms after 2030; mandatory phase-out by 2035
- NSA CNSA 2.0: All new national security system acquisitions quantum-safe by January 1, 2027
- Executive Order 14306 (June 2025): Federal quantum-safe cryptography requirements

4. Lack of Crypto-Agility

- Design systems so algorithms are configuration, not code
- Allows future swaps without re-engineering
- Example: Systems built in 2026 with hardcoded RSA-2048 can't migrate without code rewrite

Cryptographic Blind Spots

1. Invisible Cryptography

- Legacy systems, unmanaged IoT/OT devices, and cloud assets often use hardcoded or outdated encryption that is not documented

2. Untracked Data In-Transit

- Massive volume and variety of real-time data flows (East-West and North-South) often mask the use of vulnerable encryption protocols (like old TLS/SSL versions) which are not actively inventoried

3. Lack of Agility and Scale

- Size of the modern enterprise, combined with a lack of tools for rapid, orchestrated cryptographic change, means that manual, large-scale PQC migration is currently infeasible

Upgrade requirements

<u>Algorithm</u>	<u>Purpose</u>	<u>Replaces</u>	<u>Status</u>
ML-KEM (CRYSTALS-Kyber)	Key encapsulation / key exchange	RSA, DH, ECDH	Finalized FIPS 203 (August 2024)
ML-DSA (CRYSTALS-Dilithium)	Digital signatures	RSA, ECDSA, DSA	Finalized FIPS 204 (August 2024)
SLH-DSA (SPHINCS+)	Digital signatures (hash-based)	RSA, ECDSA (diversity)	Finalized FIPS 205 (August 2024)
ML-KEM + hybrid	Transitional key exchange	Running DH/ECDH + ML-KEM in parallel	Recommended 2026–2027 approach

Recommended Next Steps

1. Conduct cryptographic inventory
2. Categorize by risk (public-facing, long-lived data, regulatory sensitive)
3. Engage vendor roadmaps (OpenSSL, Java, Python, Go, cloud providers)
4. Pilot hybrid deployment on non-critical systems
5. Phase migration across risk tiers; monitor NIST/NSA guidance updates

Rapidly Close The Gap with Armis

Utilize AI/ML to automatically generate real-time...

- Deep situational awareness of every networked asset and how it communicates
- Persistent Cryptographic Bill of Materials (CBOM) for data in motion and at rest
- Timely reports/alerts on cryptographic gaps for all stakeholders
 - PMOs
 - Operators
 - Mission Commanders

Bottom Line...

Post-Quantum Cryptography is yesterday's problem...and
we're already way late to the battle.

Questions?