DELL Technologies

Post-Quantum Cryptography

Get Started

Introduction

Quantum computing is driving a fundamental redesign of technology, creating both incredible opportunities and new challenges. While this future is exciting, it introduces a significant threat to the cryptographic systems that protect our digital world.

Why is Quantum Computing on the Rise?

Classical computers, whether in laptops, smartphones, or servers, process information using bits, which exist in a state of either zero or one. This binary model has powered decades of progress, but it limits how information can be represented and manipulated. Quantum computers use qubits, which can exist in multiple states simultaneously through principles like superposition and entanglement. This allows quantum machines to explore vast numbers of possible solutions in parallel, providing a computational advantage for specific classes of problems.

What is Post-Quantum Cryptography?

Post-Quantum Cryptography (PQC) refers to a new generation of algorithms designed to secure digital systems against both classical and quantum attacks. Unlike quantum key distribution, which requires specialized hardware, PQC is designed to run on today's classical infrastructure – servers, endpoints, networks – making it the most practical and scalable way to prepare for the quantum era.

What Immediate Risks Do Organizations Face from Quantum Computing?

The consequences extend far beyond theoretical risk. Organizations that fail to prepare face exposure of sensitive intellectual property, disruption of financial systems, breaches of healthcare data, and threats to national security.

The “Harvest Now, Decrypt Later” threat compounds the urgency: adversaries need only to capture encrypted data today and wait for the means to decrypt it. By the time cryptographically relevant quantum computers arrive, the damage will already be irreversible.

“Harvest Now, Decrypt Later” – also known as “Record Now, Decrypt Later” is the act of adversaries collecting and storing encrypted data today with the intention of decrypting it in the future once cryptographically relevant quantum computers are available.

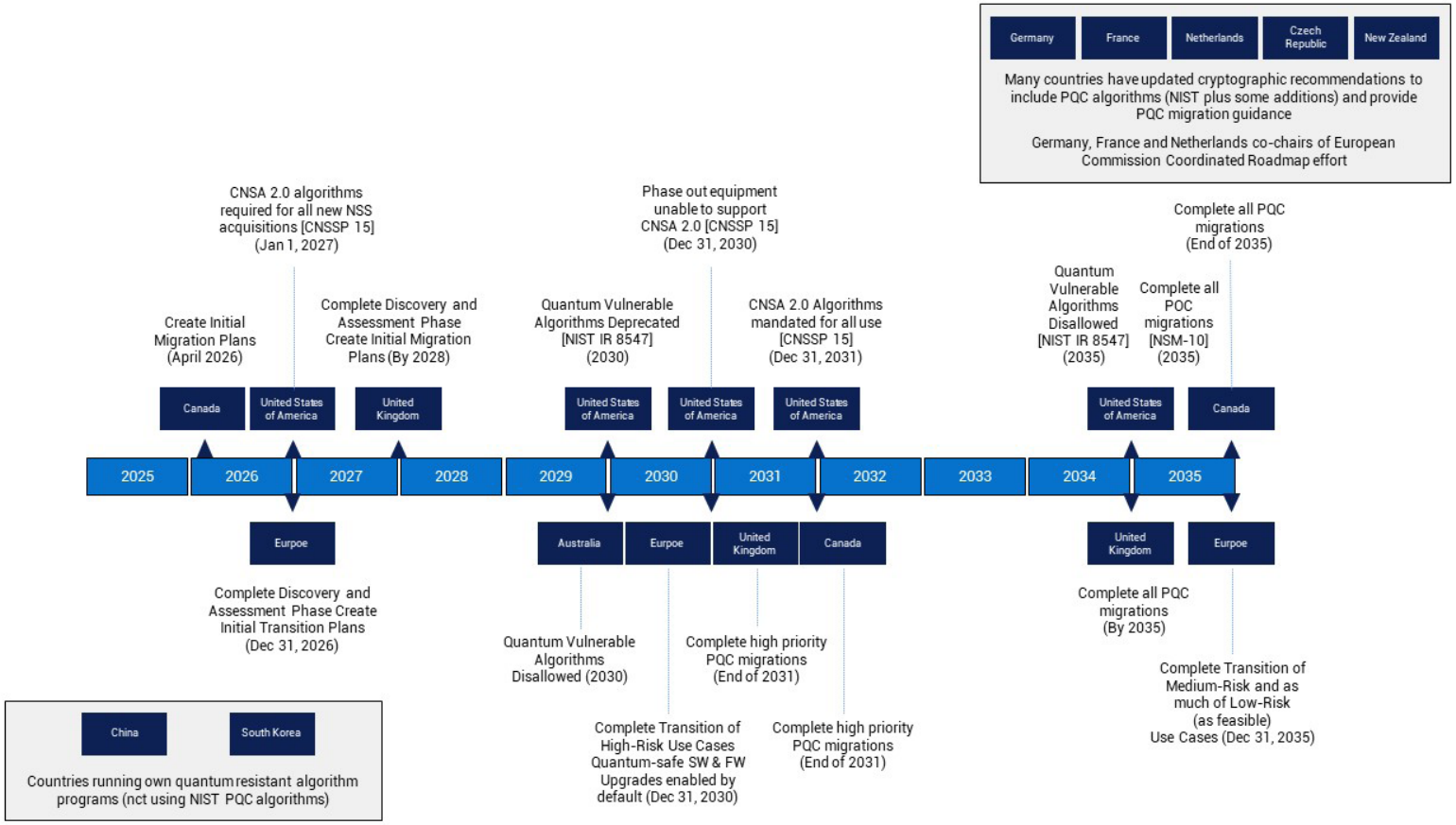
How Should Organizations Prepare for the Transition to PQC?

The journey to a quantum-safe future is a marathon, not a sprint, and an evolving journey. A proactive, layered and phased approach will help your organization manage risks, align resources, and build a resilient security posture for the long term. Dell provides the technologies and guidance to support you at every stage. Here the key steps to guide your organization in creating a PQC transition plan.

PQC Transition Timeline

Recognizing the urgency of the threat, governments and standards bodies have made PQC a global priority. Realizing the importance of adopting quantum-resistant cryptographic algorithms, the U.S. Federal Government has begun to issue PQC requirements to federal agencies. These include the National Security Memorandum 10 (NSM-10), the Commercial National Security Algorithm Suite (CNSA 2.0), the Office of Management and Budget Memorandum 23-02 (OMB M-2302), and National Institute of Standards and Technology Interagency Report 8547 (NIST IR 8547) as well as others.

Other organizations around the globe have also set guidelines for the PQC transition. These dates are not arbitrary – they reflect the lead times required to redesign, validate, and deploy cryptography across complex IT ecosystems. Enterprises should view them as more than government mandates; they are practical indicators of the global shift toward quantum resilience. Below are some of the different country mandates.



Inventory and Audit Cryptographic Threats

The first priority is to understand your current cryptographic landscape. This foundational step informs your entire migration strategy.

Good Security Hygiene

The first step in preparing for the quantum future is reinforcing the defenses already in place. Organizations should utilize strong security hygiene best practices, such as enforcing least privilege access, implementing multi-factor authentication, and maintaining rigorous patch management. There are two other considerations as well. It may be important to disable weaker cryptography such that new systems with higher cryptography can interoperate with legacy systems. It's also important, for newer systems, to raise the minimum security strength – AES-256 for symmetric cryptography, SHA-384 or higher for digests – to counter the reduced margins introduced by Grover's Algorithm. These measures not only reduce risk today but also minimize the backlog of cryptographic debt that would otherwise complicate tomorrow's migration.

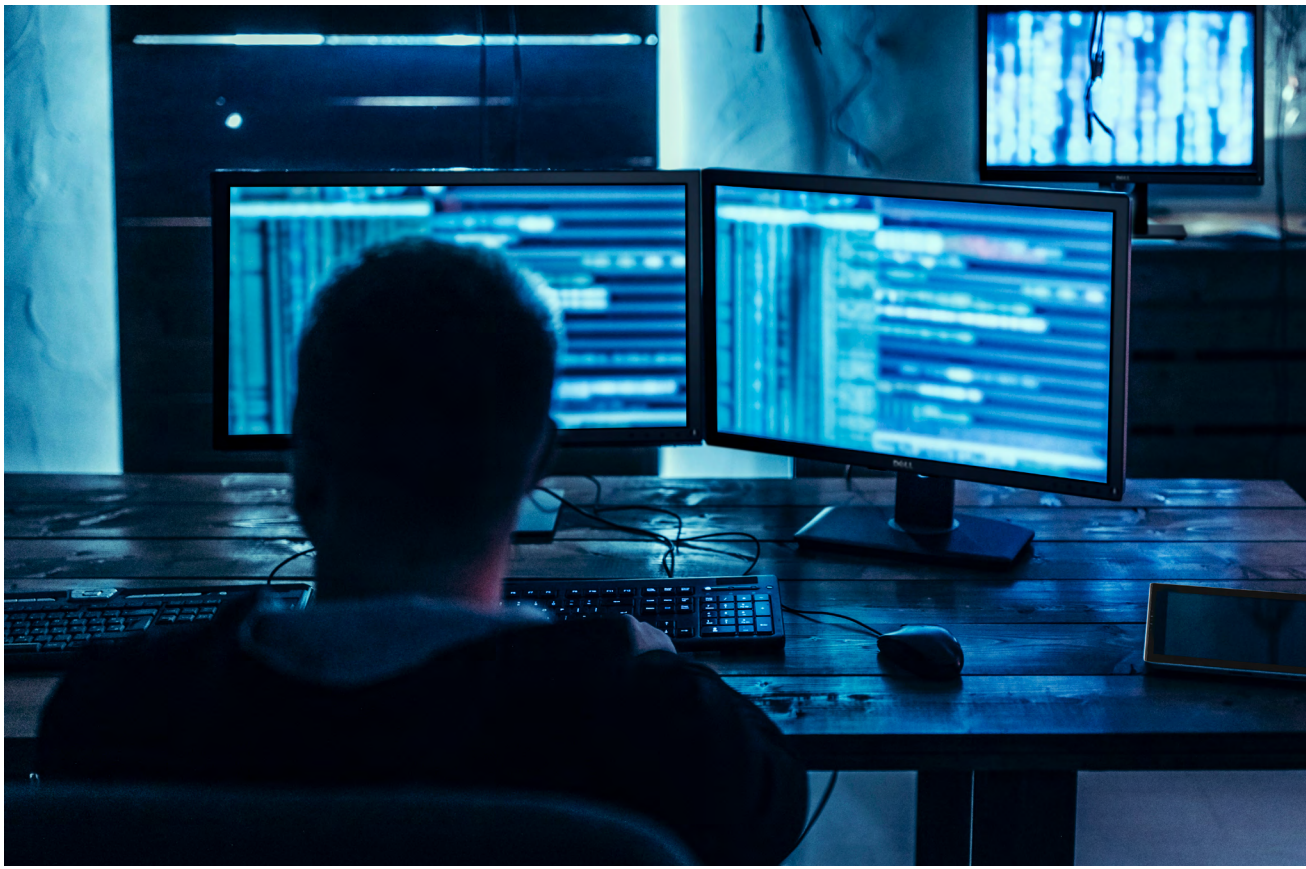
Inventory and Audit Cryptographic Assets

The cornerstone of any migration plan is visibility. Organizations must conduct a comprehensive cryptographic inventory, identifying where and how public-key cryptography is used across applications, devices, and workflows. This includes TLS certificates, VPNs, email systems, code signing mechanisms, customer data, archived data and more. Once identified, assets should be prioritized based on business criticality, sensitivity, and lifespan. Long-lived data – such as medical records or classified archives – should be treated with the highest urgency, as they are most vulnerable to the Havest Now, Decrypt Later threat.

Pilot and Experiment with PQC

With a clear inventory, you can begin hands-on experimentation with PQC-ready technologies to validate performance and integration.

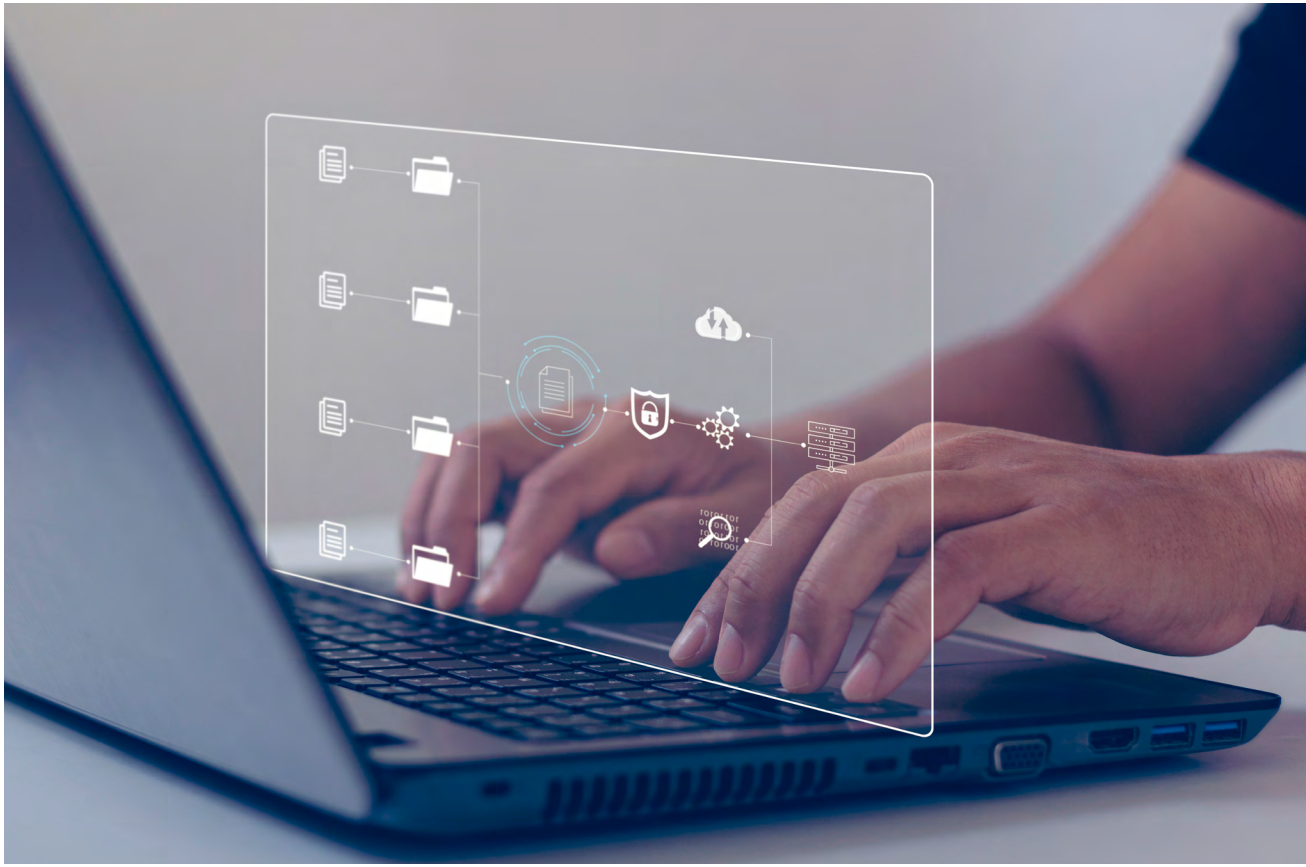
Once the cryptographic landscape is understood, organizations should begin testing PQC solutions in controlled environments. By piloting these solutions in labs, IT teams can validate performance, interoperability, and manageability before wide-scale deployment. Building this crypto agility – the ability to switch cryptographic algorithms without overhauling entire systems – is critical for long-term resilience and ease of migration.



Adopt an Interoperability Approach

As PQC standards mature, you can begin planning for production rollouts. A hybrid approach provides a bridge to a fully quantum-safe environment.

As standards mature, a hybrid model provides a bridge to the future. Many vendors are already supporting hybrid ciphersuites that combine classical and quantum-resistant algorithms in a single implementation. This dual approach provides continuity of protection even if one algorithm is later compromised. Enterprises should begin adopting hybrid strategies now, while aligning their internal timelines with their infrastructure vendor's product roadmaps and milestones. This ensures that as quantum-safe algorithms reach standardization, organizations can scale adoption without disruption.



Execute Full Migration and Continuous Validation

The ultimate goal is a fully integrated and continuously validated quantum-safe enterprise.

Execute Full Migration and Continuous Validation

The ultimate goal is a complete transition to PQC across the enterprise. This will not be a one-time event but an ongoing process of validation and adaptation. Organizations should execute detailed migration plans, incorporating PQC into every layer of their IT stack while continuously testing new standards and implementations. Using hybrid consisting of classical and quantum computers, customers can simulate attack scenarios, validate cryptographic integrity, and ensure that their systems remain resilient against evolving threats.

Collaboration and Knowledge Sharing

No organization should face this challenge alone.

Industry consortia, academic researchers, and government agencies are pooling knowledge to accelerate the PQC transition. Participation in standards groups, working groups, and pilot programs enables enterprises to stay aligned with best practices and emerging requirements. Dell's active involvement in initiatives such as the NIST NCCoE PQC project ensures our customers benefit directly from this collective expertise.

Conclusion

The quantum era is no longer a distant possibility; it is an imminent reality that requires forward-thinking action today. Preparing for this technological shift is a strategic imperative for protecting your most valuable asset—your data. As we've outlined, a phased approach that moves from inventory and auditing to full migration is the clearest path to a quantum-safe future.

The shift to PQC will be one of the most significant infrastructure changes in decades. This transition touches nearly every aspect of IT, from servers and storage to endpoints, cloud platforms, and network protocols. Success requires foresight, planning, and disciplined execution. At Dell Technologies, we see the path forward as a phased journey: one that balances immediate security improvements with long-term readiness for PQC adoption.

Dell is prepared to assist you with your strategy for implementing PQC. We recommend a phased migration plan and we have outlined a set of activities to help you strategize, plan, execute and monitor your PQC transition.