DELL Technologies

Whitepaper

Post-Quantum Cryptography: Preparing for the Quantum Era

A Dell Technologies White Paper

Table of Contents

Executive Overview

Quantum computing is moving rapidly from theoretical research to practical reality. Once considered a distant horizon, advances in hardware, algorithms, and investment are accelerating the arrival of machines capable of solving problems that classical computers cannot. The implications for industry are profound. From drug discovery to climate modeling to global logistics, quantum computing promises to unlock innovation that was previously out of reach.

But this breakthrough comes with a disruptive challenge: quantum computers will undermine the cryptographic foundations that protect the digital economy. Public-key cryptography – algorithms like RSA and elliptic curve cryptography (ECC) – has safeguarded digital communications, financial systems, healthcare records, and national security for decades. These methods rely on mathematical problems that are intractable for classical computers. Yet with the advent of cryptographically relevant quantum computers (CRQCs), these same problems can be solved efficiently, rendering today's security obsolete.

This threat is not theoretical. Some organizations are already using a tactic known as "harvest now, decrypt later" (HNDL) – collecting encrypted data today with the expectation of breaking it once quantum computers mature. Sensitive information that appears secure now may be vulnerable in a matter of years. The time to act is not when CRQCs arrive; it is today.

This white paper explains the urgency of the quantum threat, explores the emerging field of post-quantum cryptography (PQC), and provides guidance on how organizations can prepare. It highlights Dell Technologies' commitment to building a quantum-safe future – embedding security across our supply chain, hardware, firmware, software and partner ecosystem – by aligning with NIST's post-quantum cryptography (PQC) standards – FIPS 203, FIPS 204, and FIPS 205 – and with the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) guidelines. Dell's goal is clear: ensure that innovation can move forward without sacrificing security or trust.

Terminology

Throughout this paper you will encounter a number of terms. We have tried to outline some of these terms in order to help the understanding of the paper.

Post-Quantum Cryptography – A new mathematical approach to cryptography, with new algorithms, meant to be secure against quantum computer attacks. These algorithms run on classical computers and they are resistant to both the quantum attack as well as known classic cryptography attacks.

Quantum-resilient – Quantum-resilient refers to systems, algorithms, or infrastructures that are designed to remain secure even in the presence of cryptographically relevant quantum computers (CRQCs). A quantum-resilient system uses post-quantum cryptography (PQC) or other protections that withstand both classical and quantum attacks, ensuring the confidentiality, integrity, and authenticity of data into the future. Other terms such as quantum-resilient and quantum-safe are also used interchangeably.

Cryptographic Agility – (sometimes referred to as crypto agility) is the ability of an organization's systems and applications to quickly and seamlessly switch cryptographic algorithms, protocols, or key lengths without requiring major redesigns or operational disruptions.

"Harvest Now, Decrypt Later" (HNDL) – 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 (CRQCs) are available.

Quantum Computing & the Threat to Encryption

The Rise of Quantum Computing

As we described in our blog post, Post-Quantum Cryptography: A Strategic Imperative for Enterprise Resilience, almost a year ago from our CTO John Roese, 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.

The potential applications of quantum computing are extraordinary. Researchers anticipate breakthroughs in pharmaceuticals by simulating molecular interactions with precision that classical computers cannot achieve. Climate scientists envision more accurate models of global systems, while the energy sector sees potential for optimizing power grids and storage. Even logistics and manufacturing stand to benefit from quantum optimization techniques. The benefits are real and within reach – but so are the risks.

Why Encryption Is at Risk

Encryption underpins trust in the digital age. When you enter a credit card number, log into a secure website, or receive a signed software update, cryptography ensures confidentiality, authenticity, and integrity. Most of this protection relies on public-key cryptography – algorithms like RSA and ECC that are based on mathematical problems considered computationally infeasible for classical machines.

Quantum computing changes this equation. Using **Shor's Algorithm,** a sufficiently powerful quantum computer can solve the factorization and discrete logarithm problems that give RSA and ECC their strength. Once CRQCs exist, the digital signatures that protect software updates, the keys that establish TLS sessions, and the certificates that authenticate devices can all be compromised. The impact is systemic, threatening the very mechanisms that make digital transactions safe.

Symmetric cryptography – algorithms like AES used to protect stored data or secure communications – faces a different, though less severe, challenge. **Grover's Algorithm** allows a quantum computer to reduce the effective strength of symmetric keys, effectively halving their security. While this can be mitigated by moving to larger key sizes such as AES-256, the adjustment underscores the pervasive reach of quantum threats

Urgency and Consequences

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" strategy compounds the urgency: adversaries need only to capture encrypted data today and wait for the means to decrypt it. By the time CRQCs arrive, the damage will already be irreversible.

Post-Quantum Cryptography and Emerging Standards

Defining 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.

The foundation of PQC is a set of mathematical problems that, to the best of current knowledge, are resistant to quantum techniques like Shor's and Grover's algorithms. Lattice-based cryptography, hash-based signatures, code-based schemes, and multivariate equations represent the most promising families. These approaches are being rigorously tested and standardized to ensure they provide the same reliability and interoperability that RSA and ECC once delivered.

The Global Standardization Effort – Emerging Industry Standards

Recognizing the urgency of the threat, governments and standards bodies have made PQC a global priority. The U.S. National Institute of Standards and Technology (NIST) launched its PQC project in 2016, calling on the cryptographic research community to propose, analyze, and refine candidate algorithms. After years of testing, NIST announced the first group of standardized algorithms in August 2024:

- **CRYSTALS-**Kyber for public-key encryption and key establishment
- **CRYSTALS-**Dilithium and SPHINCS+ for digital signatures

Additional algorithms remain under review to provide diversity and flexibility for different implementation needs, including lightweight systems such as embedded firmware. This evolving standardization process ensures that organizations worldwide have a clear path to adopting quantum-resistant solutions.

NIST Standards – FIPS 203, 204, 205

In August 2024, the U.S. National Institute of Standards and Technology (NIST) finalized the first PQC algorithms:.

- FIPS 203 (ML-KEM) – based on CRYSTALS-Kyber, a key encapsulation mechanism. Provides IND-CCA2 security, meaning ciphertexts remain indistinguishable even under adaptive chosen-ciphertext attacks.
- FIPS 204 (ML-DSA) – based on CRYSTALS-Dilithium, a digital signature algorithm. Delivers strong EUF-CMA security (existential unforgeability under chosen-message attacks), the standard requirement for digital signatures.
- FIPS 205 (SLH-DSA) – based on SPHINCS+, a hash-based signature scheme. Selected as a conservative fallback not dependent on lattice problems.

A Mandated Roadmap

Realizing the importance of adopting quantum-resistant encryption 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 National Institute of Standards and Technology (NIST) Interagency Report (IR) 8547, and the Office of Management and Budget Memorandum 23-02 (OMB M-2302) as well as others.

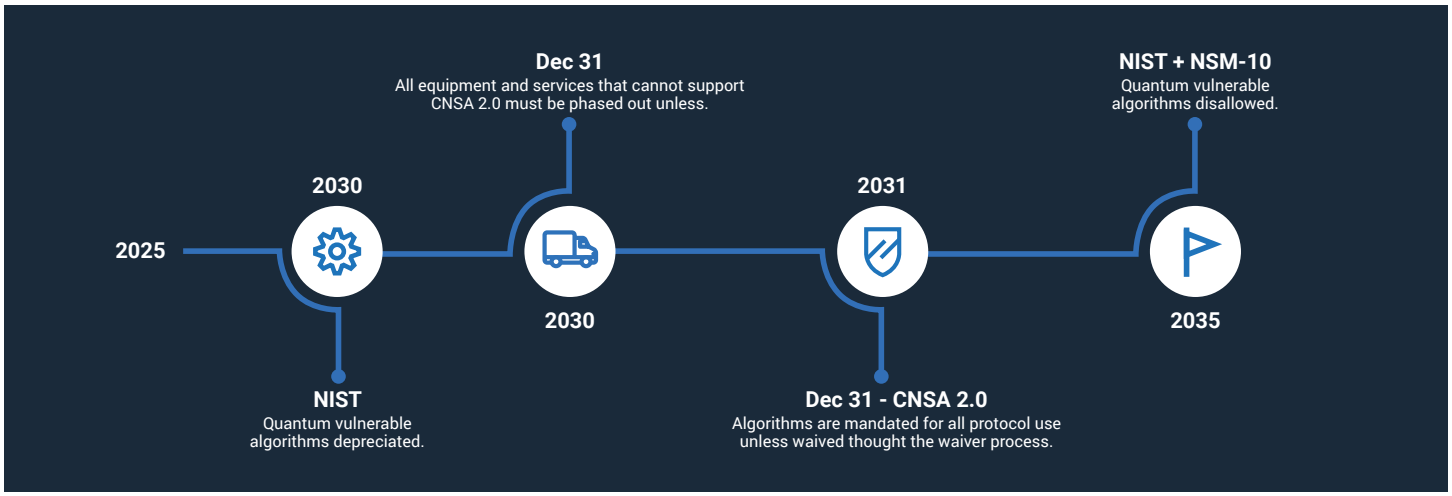
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodogies.

Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)
Introduces the first recommendations post-quantum cryptographic algorithms

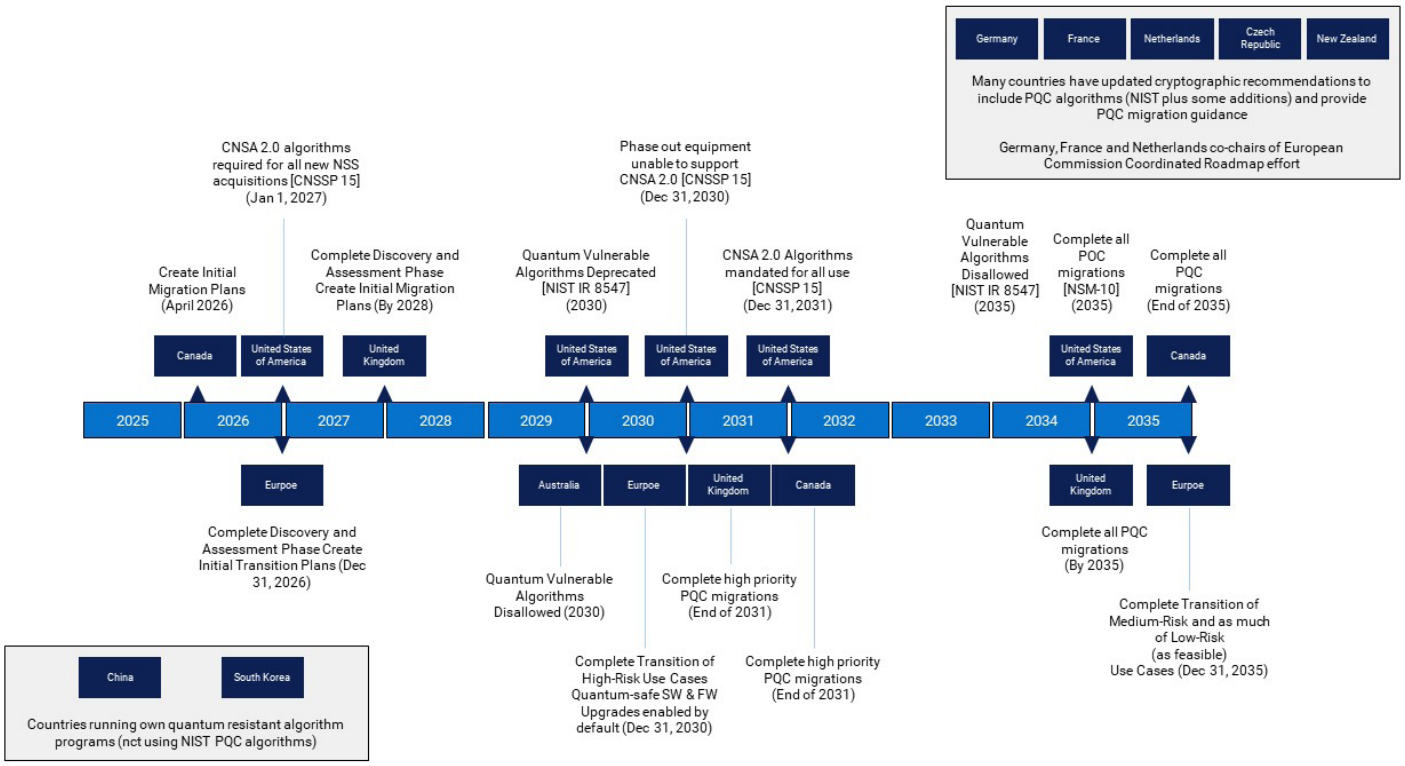
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

OMB Memorandum 23-02 (OMB M-23-02)
Provides detalied guidelines for federal agencies to how to comply with NSM-10

CNSA 2.0, announced by the NSA in September 2022, introduces the first recommendations for post-quantum cryptographic algorithms. CNSA 2.0 sets explicit deadlines for adopting quantum-resistant algorithms across National Security Systems (NSS), and it serves as a powerful guidepost for enterprises preparing their own transitions:



Other organizations around the globe have also set guidelines for the PQC transition. Below are some of the different country mandates.



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.

Industry Collaboration

Beyond NIST and NSA, Dell is actively influencing and participating in industry consortia and standards groups who are driving interoperability and adoption. The Trusted Computing Group is integrating PQC into the trusted platform module (TPM) standard. The IETF which is driving a lot of the integration of the PQC algorithms into industry protocols such as TLS, X.509 certificates for example. The OASIS Key Management Interoperability Protocol (KMIP) committees are enabling PQC for key management frameworks. The FIDO Alliance is studying PQC's impact on authentication and device onboarding standards, while organizations like SAFECode are working to educate the industry on migration preparedness.

The NIST National Cyber Security Center of Excellence (NCCoE) is the construct that allows NIST to work with industry, academia, and the government agencies via domain focused projects. They have been focusing on a number of things such as:

- Cryptographic Discovery – identifying what crypto needs to be migrated and how to prioritize what to migrate first.
- Interoperability – ensuring popular cryptographic features and protocols are incorporating the new PQC algorithms and that implementation from different vendors interoperate.
- Crypto Agility– focusing on developing information systems that encourage support of rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure, otherwise known as cryptographic agility

These projects help to inform/develop the guidance and standards that they create and help to ensure there are example industry solutions for the standards and guidance they provide. Dell has been participating in the NCCoE Migration to PQC project since its inception.

Today PQC is not just a research topic; it is a developing standard with concrete algorithms, timelines, and adoption pathways. Organizations that begin preparing now can avoid the cost, disruption, and risk of a last-minute scramble. The transition is not simply about compliance – it is about ensuring that trust, confidentiality, and integrity remain intact as quantum computing reshapes the digital landscape.

Why the Time to Act Is Now

The Immediacy of the Threat

It may be tempting to view quantum computing as a distant risk, something that can be addressed once the technology is fully realized. In reality, the clock has already started. Sensitive information – financial transactions, healthcare records, intellectual property, or government communications – may be securely encrypted today, but once quantum machines reach the threshold of breaking RSA or ECC, that data can be retroactively exposed. The result is that an entire backlog of historical communications and records could suddenly be at risk.

Long Technology Cycles

Modern IT ecosystems are not easily or quickly transformed. Historically, single algorithm replacements, such as the transition from SHA-1 to SHA-2 or DES/3DES to AES, have taken 10+ years to complete. These algorithms are deeply embedded into operating systems, applications, network devices, and hardware. Replacing them requires redesign, validation, testing, and deployment across environments that span from data centers to cloud platforms to edge devices. For many organizations, this will take years – far longer than the remaining window before quantum computing poses real-world threats. This is why regulators, standards bodies, and security leaders stress immediate preparation. Waiting until CRQCs are widely available will leave no time for an orderly transition.

Risks of Inaction

The consequences of delaying migration extend beyond technical exposure:

- Data Security Risk: Long-lived data such as medical histories, financial records, or defense information may be compromised retroactively once quantum computers mature.
- Software Authenticity and Integrity Risk: Software authenticity and integrity may be compromised with malicious code if signed with current signing methods and still in use once quantum computers mature.
- Operational Risk: Critical infrastructure systems – like utilities, transportation networks, and emergency services – are notoriously difficult to upgrade. Failure to plan now could mean operational disruption later.
- Regulatory and Compliance Risk: Frameworks like **CNSA 2.0** have established clear timelines for compliance. Organizations that fail to prepare risk not only exposure but also non-compliance with government or industry expectations.
- Reputational and Financial Risk: A breach resulting from unaddressed cryptographic vulnerabilities could lead to lasting damage to brand trust, alongside significant financial losses.

The Case for Proactive Action

Proactive preparation is not merely a defensive move; it is an opportunity to strengthen long-term resilience. By conducting cryptographic inventories, upgrading symmetric key lengths, piloting PQC-ready solutions, and engaging with vendors who offer quantum resistant offerings, organizations can ensure continuity of trust. Early adopters are better positioned to future-proof operations, maintain compliance, and demonstrate leadership to customers, partners, and regulators.

Dell's Approach to Post-Quantum Cryptography

At Dell, we believe technology drives human progress, and security is the foundation of that progress. As a company, Dell Technologies is ensuring that its portfolio, IT infrastructure, and lifecycle support systems are well-prepared for the transition to quantum resistant algorithms. Steps being taken to prepare for the transition include:

- Identifying the specific areas and purposes where cryptography is employed in products, services, IT infrastructure, and support systems to formulate comprehensive transition plans.
- Enhancing internal knowledge about Post Quantum Cryptography (PQC) algorithms, considering implementation aspects and design principles related to crypto agility to facilitate a smooth transition to PQC algorithms.
- Evaluating the performance, applicability, and suitability of PQC algorithms in various use cases relevant to Dell Technologies diverse portfolio.

Given the complex nature of the PQC transition, upgrades of the cryptographic use cases may be phased into Dell Technologies offerings. By way of example, from a data perspective, transition priority is given to use cases that could be vulnerable to 'harvest now, decrypt later' attacks such as data in flight or at rest encryption.

When considering your technology platform, transition of a cryptographic use case could involve a full product refresh/ replacement or a product upgrade. This will depend upon the product in question and where and how the cryptography is implemented in that product and surrounding systems.

Release of quantum resistant offers will be a focus over the next 5+ years to ensure that customers can meet the PQC transition timelines that are being published by governments and industry associations that fall between 2027 and 2035.

Customers should work with their Dell Account team to obtain product specific details (e.g., release roadmaps and timelines) to incorporate into their migration plans. Stay tuned as Dell will be delivering more specific timelines for PQC integration into their product lines and products in the upcoming months.

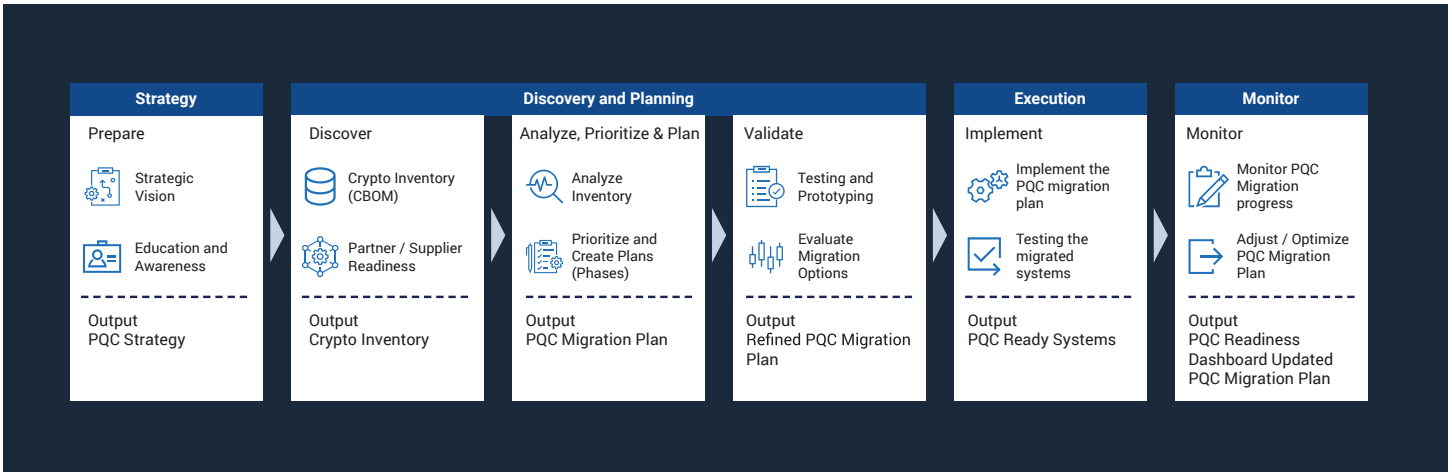
Preparing for Quantum-Resilient Innovation

Dell's goal is not only to help customers comply with emerging standards, but also to empower them to innovate securely in the quantum era. Whether deploying AI workloads, managing hybrid cloud environments, or modernizing edge infrastructure, customers can feel secure that Dell solutions are designed with resilience in mind. Security is not bolted on after the fact – it is engineered into every layer of Dell's portfolio, ensuring that organizations can navigate the transition to post-quantum cryptography with confidence.

Preparing for the Transition

The shift to post-quantum cryptography 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 migration.



Prepping Today's Security Posture

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 that symmetric cryptography, for newer systems, be upgraded to longer key lengths – AES-256 and SHA-384 or higher – 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, and archived data. 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 harvest-now, decrypt-later threat.

Pilot and Experiment with PQC

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 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 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 quantum-classical labs, customers can simulate attack scenarios, validate cryptographic integrity, and ensure that their systems remain resilient against evolving threats.

Collaboration and Knowledge Sharing

Finally, 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.

Preparing for PQC is a marathon, not a sprint. By taking a phased approach – reinforcing today's defenses, auditing cryptographic assets, piloting PQC, adopting hybrid strategies, and executing a full migration – organizations can move confidently toward quantum resilience. With Dell as a partner, this journey is not only achievable but an opportunity to strengthen trust and enable innovation well into the future.

Real-World Applications & Benefits

The transition to post-quantum cryptography is more than a compliance exercise; it is a business imperative that directly impacts trust, resilience, and long-term competitiveness. For telecommunications providers, financial institutions, healthcare organizations, and government agencies, the adoption of quantum-resistant algorithms ensures that critical digital infrastructure remains secure against both current and future threats.

Telecommunications

Telecom networks are the backbone of global digitalization. They enable everything from emergency services and IoT connectivity to secure customer communications. A quantum breach in this sector could compromise SIM provisioning, eSIM onboarding, or the authentication processes that underpin 4G and 5G. By deploying hybrid and quantum-safe cryptography now, operators can maintain customer trust, protect data privacy, and ensure seamless continuity of service across generations of mobile technology.

Financial Services

The financial industry is among the most targeted by cyber adversaries, and the integrity of transactions depends on cryptography. Post-quantum readiness safeguards digital payments, online banking, and interbank transfers against quantum-enabled fraud. Early adoption also reassures regulators and customers that institutions are committed to protecting assets and maintaining systemic stability. Future-proofing cryptography in this sector reduces both regulatory exposure and reputational risk.

Healthcare

Patient records, genomic data, and connected medical devices are all at risk from “harvest now, decrypt later” attacks. The healthcare sector faces an additional challenge: the long retention periods required for sensitive medical data. By beginning the transition to PQC today, hospitals and providers ensure that health records remain private not just now, but decades into the future. This is essential to preserving patient trust while meeting evolving data protection regulations.

Government and Critical Infrastructure

From defense communications to energy distribution systems, governments and infrastructure operators rely on cryptography for continuity of operations and national security. Post-quantum cryptography protects not only against near-term adversaries but also against the strategic collection of encrypted communications for future exploitation. Aligning with frameworks such as CNSA 2.0 ensures that government systems remain interoperable, secure, and trusted in the quantum era.

Broader Business Benefits

While the technical necessity of PQC is clear, the business case is equally strong:

- Trust and Brand Reputation: Demonstrates leadership in safeguarding customer and partner data.
- Regulatory Compliance: Aligns with NIST standards and government mandates such as CNSA 2.0.
- Operational Resilience: Reduces the risk of catastrophic outages caused by broken cryptography.
- Competitive Differentiation: Positions organizations as proactive innovators rather than reactive followers.

The benefits of acting now extend well beyond technical resilience. Organizations that embrace PQC early will not only reduce risk but also strengthen their ability to innovate, comply, and compete in a digital economy that depends on trust.

Take the Next Steps

The arrival of quantum computing represents both a generational opportunity and an unprecedented security challenge. While the exact timeline for cryptographically relevant quantum computers remains uncertain, what is certain is the effort required to prepare. Transitioning to post-quantum cryptography will take years of coordinated planning, investment, and execution. Waiting until quantum computers are operational is not a practical option.

The first step for any organization is awareness: understanding where and how cryptography is used across their environment. From there, enterprises must begin the process of inventorying, prioritizing, and piloting quantum-safe solutions. Hybrid cryptography – combining classical and post-quantum algorithms – provides an immediate path to resilience while standards continue to evolve. By aligning internal roadmaps with global frameworks like NIST's PQC standards and CNSA 2.0 timelines, organizations can move confidently toward compliance and interoperability.

Dell Technologies is committed to helping customers navigate this transition. Through our approach, we provide a foundation of supply chain integrity, hardware-embedded safeguards, and software-enabled adaptability. Our partnerships with leading security providers and our active role in industry standards bodies ensure that Dell solutions are not only aligned with the latest requirements but also tested for real-world performance and interoperability.

Begin preparing today. Start with discovery and risk analysis, engage with trusted vendors, and pilot quantum-safe technologies. Every step taken now reduces the risk of disruption tomorrow. Organizations that act early will not only secure their data and systems but will also earn the trust of customers, regulators, and partners in an era where digital confidence is paramount trust.

About Us

Dell Technologies is committed to making advanced technology accessible, trustworthy, and empowering for everyone. We help people and organizations safely harness innovation, leading the way toward a more secure, inclusive, and connected future.