Commvault

EXECUTIVE BRIEF

Protecting Your Data: Why Post-Quantum Cryptography Matters

Executive Brief for Senior IT and Security Leaders

THE QUANTUM THREAT IS REAL – AND CLOSER THAN YOU THINK

We're at an inflection point with quantum computing as it homes in on becoming reality. While the potential is tantalizing, it also presents an unprecedented threat to classical data security infrastructure and the cryptography algorithms that protect it.

Quantum computers leverage quantum mechanical principles to solve complex problems that classical computers cannot feasibly address. Of particular concern is their ability to break widely used public key encryption algorithms like RSA and ECC (Elliptic Curve Cryptography). Once a sufficiently powerful quantum computer exists, these encryption methods – which secure virtually all digital communications today – will become obsolete.

WHY SHOULD YOU CARE NOW?

The timeline for when cryptographically relevant quantum computers will emerge remains uncertain – estimates range from 5 to 10 years. However, the risk is immediate due to "harvest now, decrypt later" attacks already underway, especially for data with longer shelf life.

Changing cryptography in a complex IT environment is not an overnight, flip-the-switch activity.

It can take years.

If your organization maintains data with long-term sensitivity – intellectual property, trade secrets, financial information, or personal data – this represents a significant and growing risk.

THE STAKES: YOUR MOST VALUABLE DIGITAL ASSETS

Consider what's at stake:

- **Intellectual property protection:** Trade secrets, research data, financial records, and proprietary algorithms could be exposed, destroying competitive advantages built over decades.
- **Data privacy and compliance:** Sensitive personal information could be decrypted, potentially leading to massive compliance violations under GDPR, HIPAA, and other regulations.
- **Authentication systems:** Digital signatures and identity verification methods could be compromised, undermining zero-trust architectures and enabling sophisticated impersonation attacks.
- **Secure communications:** TLS/SSL protocols that secure communications could be broken, exposing confidential information in transit.

The financial, operational, and reputational damage from such exposures could be catastrophic – and unavoidable without proactive measures.

POST-QUANTUM CRYPTOGRAPHY: THE PATH FORWARD

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to be secure against attacks from both classical and quantum computers. These algorithms rely on mathematical problems that remain difficult even for today's quantum computers to solve.

In 2024, the National Institute of Standards and Technology (NIST) published its first set of standardized post-quantum cryptographic algorithms, including CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+. With these standards now available, organizations can begin implementing quantum-resistant cryptography.

Key steps in your post-quantum transition should include:

1. **Cryptographic inventory:** Identify where cryptography needs to be used across your digital estate. This should include your most sensitive data – applications, networking, identity systems, data-at-rest protection, and third-party connections.
2. **Risk assessment:** Given the cost of overhead for PQC, it makes sense to prioritize protecting your most sensitive data rather than attempting to protect everything. Evaluate your data based on sensitivity and longevity. Information that must remain confidential for longer than five years should have your immediate attention. For less sensitive data, standard encryption methods should be relatively safe.
3. **Crypto-agility implementation:** Develop frameworks that allow you to quickly replace cryptographic algorithms without major system redesigns. Hybrid classical/PQ deployment must balance cost and complexity, but opportunity costs in finance and healthcare are high. Crypto agility also requires employee enablement.
4. **Prioritized migration:** Begin with your most sensitive systems and data, particularly those securing intellectual property or personally identifiable information.
5. **Vendor engagement:** Confirm all vendors in your ecosystem are aligned with emerging standards to avoid rework.

HOW COMMVAULT IS LEADING THE WAY

Commvault has been at the forefront of PQC implementation, recognizing early the critical threat quantum computing poses to data security. As organizations entrust us with their most valuable asset – their data – we've taken proactive steps to protect it against both current and future threats:

- **Crypto-agility:** Our solutions are designed with crypto-agility in mind, allowing for rapid adaptation as PQC standards evolve and new algorithms emerge.
- **Optimized approach:** We utilize both traditional encryption (AES-256) and post-quantum algorithms to provide defense-in-depth against both classical and quantum threats.

Commvault's PQC capabilities are available in Commvault Cloud Platform Release 2024E and later versions.

THE TIME TO ACT IS NOW

As noted earlier, migration to PQC will take significant time – potentially years for large organizations with complex IT environments. Historical precedent shows that major cryptographic transitions typically require 5 to 10 years to complete. Commvault's aim is to make enabling this in our solution as simple as possible for customers.

By beginning your post-quantum transition today, you can help protect your organization's most valuable data as we enter the quantum era. The alternative – waiting until quantum computers break existing encryption – will be too late for data that has already been compromised.

Commvault stands ready to help you navigate this transition, providing the technology, expertise, and guidance needed to help secure your data for the quantum future.

For more information on Commvault's PQC implementation and how we can help your organization prepare for quantum threats, contact your Commvault representative or visit **commvault.com.**