Futurum

NetApp®

Secure Data Infrastructure in a Post-Quantum Cryptographic World

APRIL 2025

Executive Summary

Within the next 5 to 10 years, quantum computers may become powerful enough to break many classical forms of encryption. Organizations must start preparing now to safeguard their infrastructure, especially data and storage. Those that do not would risk having their confidential information stolen now and decrypted later and running out of time to migrate to the new quantum-safe Post-Quantum Cryptographic (PQC) protocols.

Introduction

Over 30 years ago, in 1994, Bell Laboratories mathematician Peter Shor discovered a new algorithm for factoring large integers. While this feat was of passing and mild interest to most people who heard about it, the algorithm signaled a threat to traditional cryptographic schemes such as Rivest-Shamir-Adleman (RSA), which have been in use since the 1970s. The catch? Shor's approach not only required a classical computer but also a sufficiently large quantum computer.

We would not see the first quantum computer until 1998, a tiny two "qubit," or "quantum bit," device. Even in 2025, the quantum computers we see from any of the 80+ companies, such as IBM and startup Quantinuum, that are developing systems are still much too small to pose a security threat. Nevertheless, there is a good chance that quantum computers will reach the size and performance levels required to break traditional forms of encryption within 5 to 10 years.

In this Futurum Market Brief, we examine this potential quantum cybersecurity threat, which encryption protocols and industries are most at risk, and Post-Quantum Cryptographic (PQC) responses by standards groups and vendors to lessen or avoid the impact. We also state what organizations must do now to protect their infrastructure, particularly those related to your data and storage.

Current Cryptographic Protocols at the Most Risk

Symmetric cryptography, which relies on the same key for encryption and decryption, is generally considered relatively low-risk and resistant to quantum computing-related threats. These approaches include the Advanced Encryption Standard with a 256-bit key (AES-256), Secure Hash Algorithm-2 (SHA-2), and Secure Hash Algorithm-3 (SHA-3). Notably, security experts currently consider hash-based algorithms post-quantum safe.

Another potential vulnerability is that AES encryption can rely on more vulnerable asymmetric encryption schemes, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) for key management and distribution. With this in mind, updating the key manager's authentication keys to PQC, specifically regarding certificate authentication, is essential to protect AES keys when on the external key manager.

Asymmetric or "public-key" algorithms rely on the computational difficulty of factoring certain large integers and are, as a result, highly vulnerable to Shor's algorithm.

Public-key cryptographic protocols are less secure and riskier from a post-quantum cryptography standpoint. These algorithms include the following:

- RSA, which is widely used and underpins digital signatures and secure communications.
- ECC, including the Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECD) Algorithms, which are used in Transport Layer Security (TLS), blockchain technologies, and secure messaging.
- Diffie-Hellman Key Exchange (DHKE), which is used for secure key exchange.
- Digital Signature Algorithm (DSA), which generates digital signatures, or cryptographic codes that prove a message originated from a specific sender and has not been altered.

The NIST Response

In August 2016, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) began an international process to "solicit, evaluate, and standardize one or more quantum-safe public-key cryptographic algorithms."[1]

After eight years of evaluating dozens of proposals, the NIST approved three such PQC standards in 2024:

- **FIPS 203:** primary standard for general encryption.
- **FIPS 204:** primary standard for protecting digital signatures.
- **FIPS 205:** alternative for protecting digital signatures.

FIPS 203 and 204 use lattice-based cryptography, and FIPS 205 uses hash-based cryptography.

Many vendors and organizations waited until NIST finalized the standards before implementing them. This is especially true for large organizations that must be FIPS compliant.

As quantum computing evolves, NIST continues to solicit and draft additional standards. Notably, in March 2025, it announced the selection of HQC as a backup algorithm to FIPS 203 for general encryption.

1 "Post-Quantum Cryptography: Proposed Requirements and Evaluation Criteria," https://csrc.nist.gov/news/2016/post-quantum-cryptography-proposed-requirements.
2 "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard," https://csrc.nist.gov/pubs/fips/203/final.
3 "FIPS 204: Module-Lattice-Based Digital Signature Standard," https://csrc.nist.gov/pubs/fips/204/final.
4 "FIPS 205: Stateless Hash-Based Digital Signature Standard," https://csrc.nist.gov/pubs/fips/205/final.
5 "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption, https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption.

Actions Being Taken Today by Bad Actors

If we do not yet have powerful enough quantum computers that can break some traditional forms of encryption, why do we care about implementing new standards and capabilities to avoid the threat?

The first reason is that it can take months to years to identify all the cryptographic uses across the organization, including hardware and software used by third parties across the supply chain. Once inventoried, risks must be remediated, which can also take years.

For example, consider all the data at rest in large organizations. To be protected in a post-quantum world, the data must be identified, classified, and possibly re-encrypted with sufficient cryptography. This will be time-consuming and require significant resources, but it must be started immediately.

The second reason is much more immediate: bad actors are collecting encrypted data today to decrypt it later when we have quantum systems with enough processing power. This can include passwords, personal information, Social Security numbers, financial data, health records, intellectual property, trade secrets, product designs, corporate and government confidential information and secrets, and military and defense classified information, to name a few.

We call these actions "Harvest Now, Decrypt Later." Some confidential data may expire, but much will remain significant for years and decades. Protecting this data today is critical to ensure that it remains encrypted in the future, even if it is stolen.

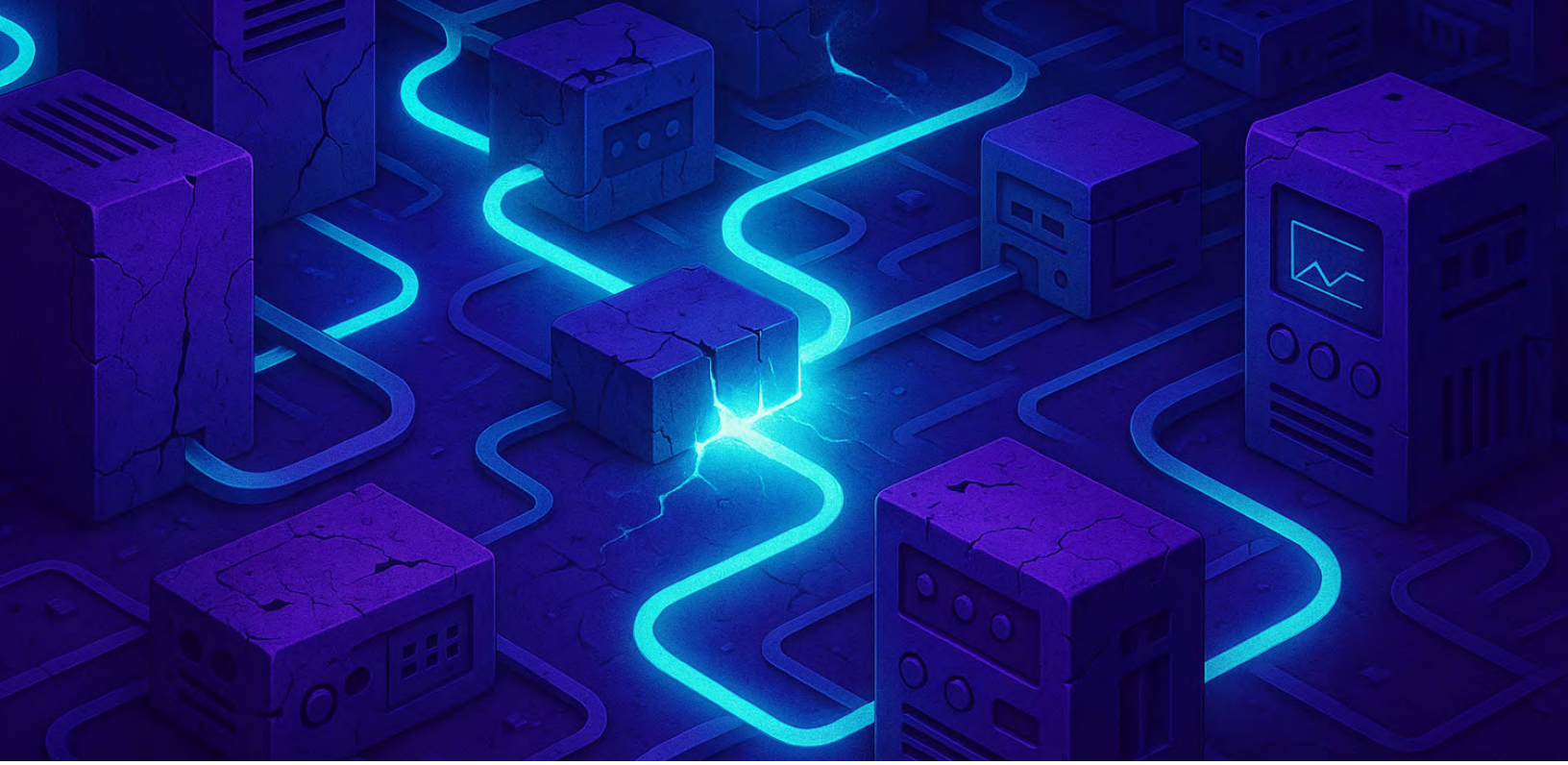
Implications for the Security of Data and Storage

Regarding data and information storage security, the vulnerability of traditional cryptography resulting from the advent of quantum computing has several implications:

- encrypted backups and archives could be exposed,
- secure communication channels and protocols could be compromised,
- data transfer and remote access could be rendered vulnerable,
- SSDs, HDDS, and other drive types not using AES-256 bit encryption are at risk, and
- encryption key management systems may be compromised.

Futurum notes that malicious attackers will likely focus first on critical infrastructure systems, which will consequently be particularly vulnerable.

Beyond intrinsic security threats, organizations that must comply with data privacy legislations such as GDPR, CCPA, and HIPAA will be required to protect sensitive data from quantum attacks.



Industry Sectors with the Most Critical Long-Term Risk

Companies across many industries are subject to risks involving losing confidential and sensitive data because of the complexity of existing security systems, the time and cost to convert to new protocols, and interconnected legacy and newer hardware. Examples of specific factors and risks in industries include:

Financial Services

High volume of data transmitted and stored, and the high value of assets subject to loss.

Healthcare and Medical Devices

Critical infrastructure and IoT devices directly affecting patient health.

Energy

Heterogeneous power sources and network interfaces.

Transportation

Economic impact due to disruptions caused by cybersecurity attacks.

Telecommunications

The impact of disruptions on other industries and their global effect.

Military and Defense

Threats to the lives of civilians and military personnel.

Government and National Security

Security of intelligence information and plans.

Intelligently Safeguarding Your Data and Storage Infrastructure

The rise of quantum computers with their potential ability to crack private keys is mandating the avoidance of classical encryption methods such as RSA, ECC, and DSA. At the same time, classical encryption methods must still be supported during the transition to PQC to support legacy systems and infrastructure, backward compatibility, and interoperability.

Key management will be critical during this gradual, phased adoption. This must include creating and securely distributing keys, managing the lifecycle of rotated and renewed encryption keys, preventing unauthorized access, and reducing exposure to quantum decryption. As systems move toward PQC algorithms, these actions ensure that old keys won't remain in use longer than necessary, decreasing their potential exposure to quantum attacks.

Organizations must migrate to PQC for data encryption at rest, in transit, and in use to ensure data security and compliance. This is needed to protect data if the physical storage device is compromised, to secure it while it is being transmitted over networks, and to prevent its exposure while it is being processed in memory.

Government Mandates to Use PQC Standards

President Biden signed the United States Quantum Computing Cybersecurity Preparedness Act into law in December 2022.[6] The law directed the Director of the Office of Management and Budget and others to issue guidance to government agencies on migrating to PQC. This included creating and maintaining an inventory of quantum-susceptible assets, prioritizing the assets to be migrated, creating a migration plan, and establishing criteria for evaluating progress. Futurum notes that companies should follow the same path. Other US federal mandates and executive orders provided greater operational details.

Australia, Canada, the Czech Republic, France, Germany, Israel, Japan, the Netherlands, New Zealand, and Spain are the most active countries in inventorying, planning, and migrating to PQC. The European Union has published a coordinated implementation roadmap.[7]

6 "H.R.7535 - Quantum Computing Cybersecurity Preparedness Act", https://www.congress.gov/bill/117th-congress/house-bill/7535.
7 "Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography," https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.

Moving to Crypto-Agility to Prepare for Future Challenges

Moving from one cryptographic protocol to another can be difficult and time-consuming. Crypto-Agility (CA) involves designing your cybersecurity infrastructure to minimize the disruption caused by such transitions:

- Don't just swap one method for another; take a broader cyber perspective to build a more flexible and comprehensive security solution.
- Take a modular approach across your infrastructure to upgrade or replace cryptographic protocols with minimal service disruption.
- Implement key rotation.
- Ensure that all uses of cryptography are known and monitored.
- Support both classical and PQC TLS connections for web applications with a fixed end-of-support date for the classical version.

Timelines and Milestones for Moving to PQC

A major corporation with broad cryptographic implementations and exposure should assume that fully migrating to PQC will take 10 years. You will be too late to start the migration process if you wait for the arrival of quantum computers that are powerful enough to break today's traditional encryption.

The process is iterative but includes the following steps in this order:

- Ensure PQC compliance with any new hardware, software, or services.
- Inventory internal infrastructure, including computing, networking, and storage.
- Inventory external access to and from internal infrastructure.
- Determine the regulatory compliance requirements that affect your timelines and other requirements.
- Prioritize assets to be protected by migrating to PQC.
- Develop the migration plan with milestones and KPIs.
- Engage with vendors and cloud providers to know and understand their migration plans and determine if they are acceptable.
- Upgrade or replace hardware to be PQC-compliant in its operation and the software it supports.
- Upgrade or replace software with PQC-compliant versions.
- Migrate systems, and periodically review progress and best practices learned during the process.
- Monitor ongoing cryptographic research to learn if anyone develops new quantum attacks on protocols such as AES.

Examples of companies that are moving to PQC include Apple with iMessage, Microsoft updating its SymCrypt library to be PQC-compliant for use across Azure and Windows, Google with its Chrome browser.

Conclusion

Skipping or delaying migration to PQC standards is no longer an option. An increasing number of IT vendors and providers are ready to assist you in the immediate crypto-agile adoption of PQC standards to protect your critical data, storage, networking, and other infrastructure from the coming quantum threat. Act now.

8 "Apple secures iMessage using post-quantum cryptography standard," Tech Monitor, https://www.techmonitor.ai/hardware/quantum/apple-post-quantum-cryptography.
9 "Microsoft Adds Support for Post-Quantum Algorithms in SymCrypt Library," Security Week, https://www.securityweek.com/microsoft-adds-support-for-post-quantum-algorithms-in-symcrypt-library/.
10 "Post-Quantum Cryptography: Standards and Progress," https://security.googleblog.com/2024/08/post-quantum-cryptography-standards.html.

Important Information About this Report

CONTRIBUTORS

Bob Sutor
Consulting Analyst | The Futurum Group

Krista Case
Research Director | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

NetApp®

ABOUT NETAPP

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data, operational and workload services to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, harnessing observability and AI to enable the industry's best data management. As the only enterprise-grade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility. In addition, our data services create a data advantage through superior cyber resilience, governance, and application agility. Our operational and workload services provide continuous optimization of performance and efficiency for infrastructure and workloads through observability and AI. No matter the data type, workload, or environment, with NetApp you can transform your data infrastructure to realize your business possibilities. Learn more at www.netapp.com or follow us on X, LinkedIn, Facebook, and Instagram.

Futurum

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

Futurum

CONTACT INFORMATION

The Futurum Group LLC | futurumgroup.com | (833) 722-5337 |