

What is Post-Quantum Cryptography?

What it means, why it matters, and how to prepare.

What you need to know

- Quantum computing is becoming a strategic cybersecurity issue, not a distant technical concern.
- Sensitive encrypted data may already be exposed through Harvest Now, Decrypt Later attacks.
- Post-quantum cryptography gives organisations a practical path to quantum-safe security.
- Senetas helps organisations start now with high-speed, crypto-agile encryption across existing infrastructure.

Introduction

Encryption underpins digital trust. It protects the data, systems and communications that governments, enterprises and critical infrastructure rely on every day.

Quantum computing changes the risk profile. A sufficiently powerful quantum computer could eventually break many of the cryptographic algorithms used today, exposing information that was assumed to be secure.

The timing is uncertain, but the direction is clear. Governments and security agencies are already preparing for the shift to post-quantum cryptography. For leaders, the priority is not to predict the exact arrival of quantum capability — it is to reduce exposure and start planning now. Senetas helps organisations take that first step with high-speed, crypto-agile encryption designed for the post-quantum era.





The world we live in today

The modern digital economy depends on cryptography. It helps protect:

- Sensitive government information
- Healthcare records
- Financial transactions
- Defence communications
- Intellectual property
- Customer and employee data
- Critical infrastructure networks

Most of this protection relies on cryptographic algorithms developed decades ago. They remain highly secure against today's computers, which is why they have become global standards. The challenge is that they were not designed with quantum computing in mind.

What changes in a quantum world?

Quantum computers process information differently from traditional computers. While classical computers solve problems through sequential calculations, quantum computers can perform certain types of calculations exponentially faster.

For cybersecurity, this matters because many encryption standards rely on mathematical problems that are extremely difficult for traditional computers to solve. A sufficiently powerful quantum computer could solve some of these problems in a fraction of the time, potentially allowing encrypted information to be decrypted.

This is why governments, regulators and security agencies are treating quantum readiness as a strategic cybersecurity priority, not a future technical issue.

The threat is not just future quantum computers

One of the most important concepts to understand is **Harvest Now, Decrypt Later attacks (HNDL)**. This assumes attackers do not need a quantum computer today to create a future risk. They can capture encrypted data now, store it and decrypt it later when quantum capabilities become available.

Why the risk starts now:

If data must remain confidential for five years or more, it is already exposed. Information stolen today can be decrypted once a cryptographically relevant quantum computer exists.

Security researchers and government agencies have increasingly warned organisations of this risk, particularly where national security, defence, critical infrastructure and financial services data are concerned. For many organisations, the quantum challenge has already begun.

What is Post-Quantum Cryptography?

Post-quantum cryptography, or PQC, is a new generation of cryptographic algorithms designed to resist both classical and quantum attacks.

For executives, the key point is simple: PQC is not quantum technology. It is a practical security transition that can run across existing infrastructure and help protect sensitive data before quantum threats become operational.

Senetas enables that transition with certified, high assurance network encryption that supports quantum-safe protection without forcing a rip-and-replace program. This gives organisations a way to reduce risk now while preparing for evolving standards and compliance expectations.

What to be thinking about today

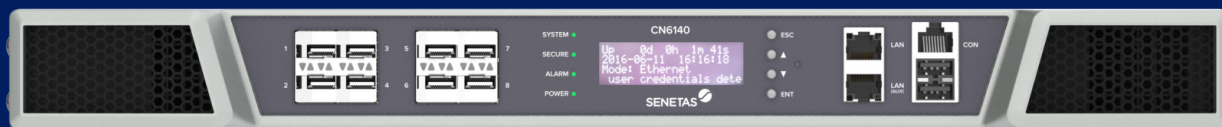
There are five priorities:

- Know where cryptography is used across the organisation.
- Identify systems protecting long-life sensitive data.
- Assess exposure to quantum-related threats and harvest-now-decrypt-later risk.
- Build a phased migration roadmap.
- Prioritise crypto-agile technologies that can adapt as standards evolve.

The Senetas approach supports hybrid deployment, enabling classical and post-quantum encryption to operate together so organisations can start reducing risk while migrating in a controlled way.



One consistent encryption layer across core, branch, cloud, tactical and partner connectivity. Every Senetas network encryption device is PQC-ready, interoperable and centrally managed from one platform — whatever the mix.



Actions to take now

Quantum readiness should start with a practical, staged plan:



Assess exposure

Identify where cryptography is used, prioritise data that must remain confidential for five years or more, and assess HNDL risk.



Test hybrid protection

Pilot classical and post-quantum encryption in controlled environments to validate performance, interoperability and operational impact.



Build the roadmap

Define a phased migration plan that prioritises critical systems, crypto-agile technology and future compliance requirements.

Talk to Senetas now

Quantum readiness starts before quantum disruption arrives. Speak to Senetas about assessing your exposure, protecting sensitive data in motion and building a practical path to post-quantum security.

[Contact us](#)

Senetas Corporation Limited

312 Kings Way, South Melbourne, VIC 3205, Australia | **T** +61 03 9868 4555 | **E** info@senetas.com | ABN 33 006 067 607

senetas.com

03092026