SSH | Defensive Cybersecurity

Post-Quantum Cryptography

Prepare for a quantum-safe future today.

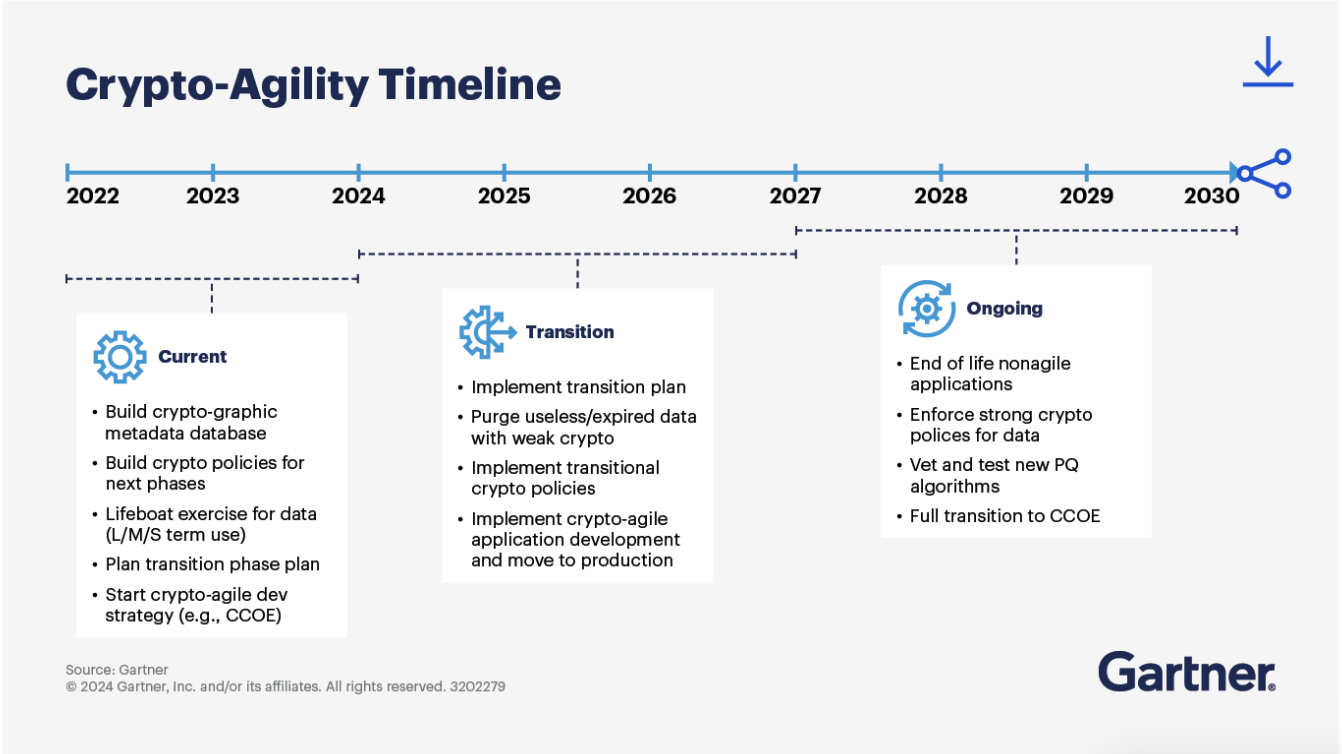
What did Gartner say?

Begin Transitioning to Post-Quantum Cryptography Now

Quantum computing will render traditional cryptography unsafe by 2029. It's worth starting the post-quantum cryptography transition now.

By **Mark Horvath** | September 30, 2024

*This page features a previous edition of Gartner's Top Strategic Technology Trends. For the most up-to-date insights, explore the **Gartner Top 10 Strategic Technology Trends for 2026**.*

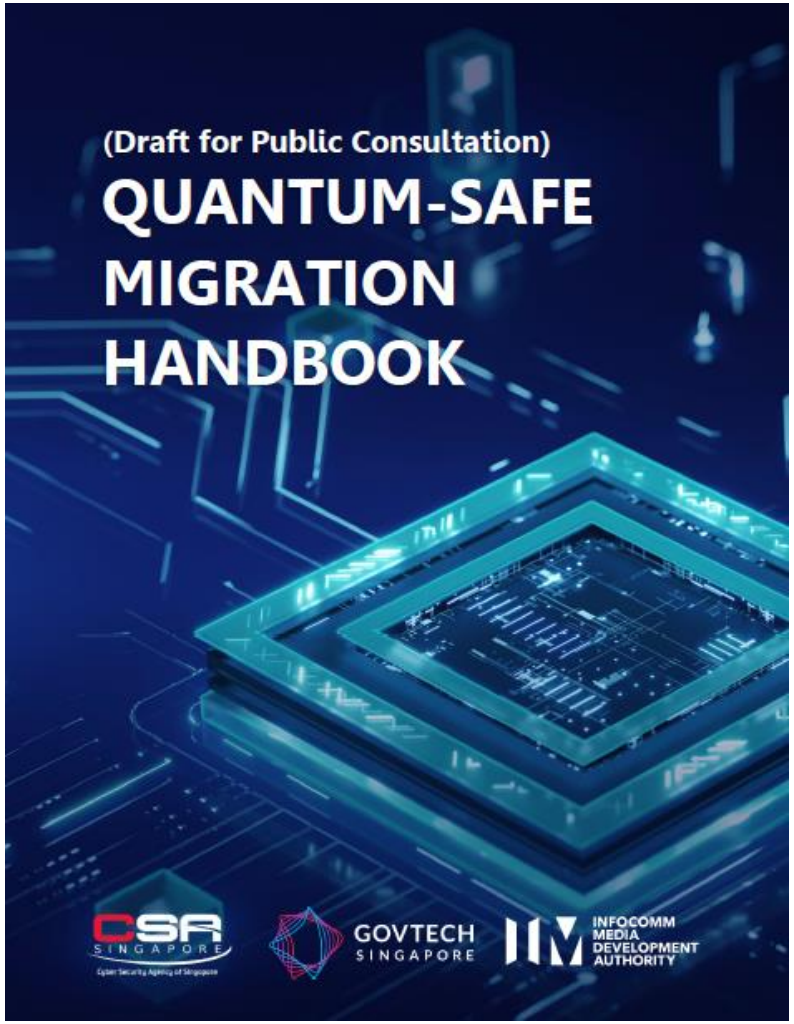


https://www.gartner.com/en/articles/post-quantum-cryptography

SSH

Cyber Security Agency (CSA)

- Quantum-Safe Migration handbook from CSA
- Issued: 23rd Oct 2025

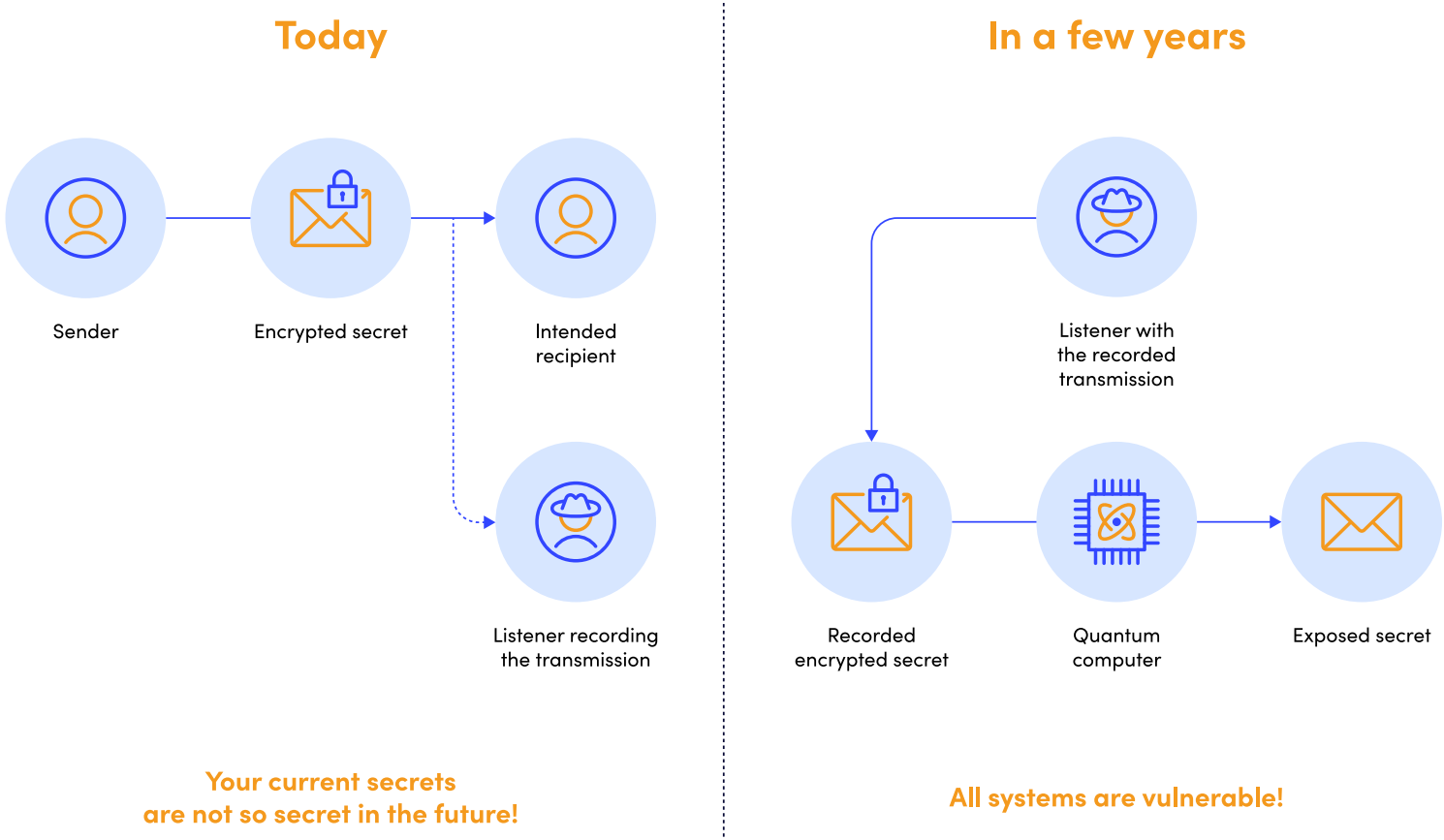


Quantum-safe Migration

Key takeaways:

1. Q-day is a when and not an if – organisations should start preparing and planning now as it will take significant effort and time to migrate.
2. However, there is no need to rush into implementation too quickly, as the quantum-safe solution space is still developing. Use the time to seed readiness and build capability.

Quantum Computers are not widely available yet – Why bother now?



Record Now, Decrypt Later

Consider any important secret that needs to be protected for a long time:

- **Health information**
- **Personal IDs**
- **Diplomatic secrets**
- **Military secrets**

By recording and storing encrypted communications now, threat actors can decrypt the message with quantum computers in the future.

SSH

Regulatory push & global timelines

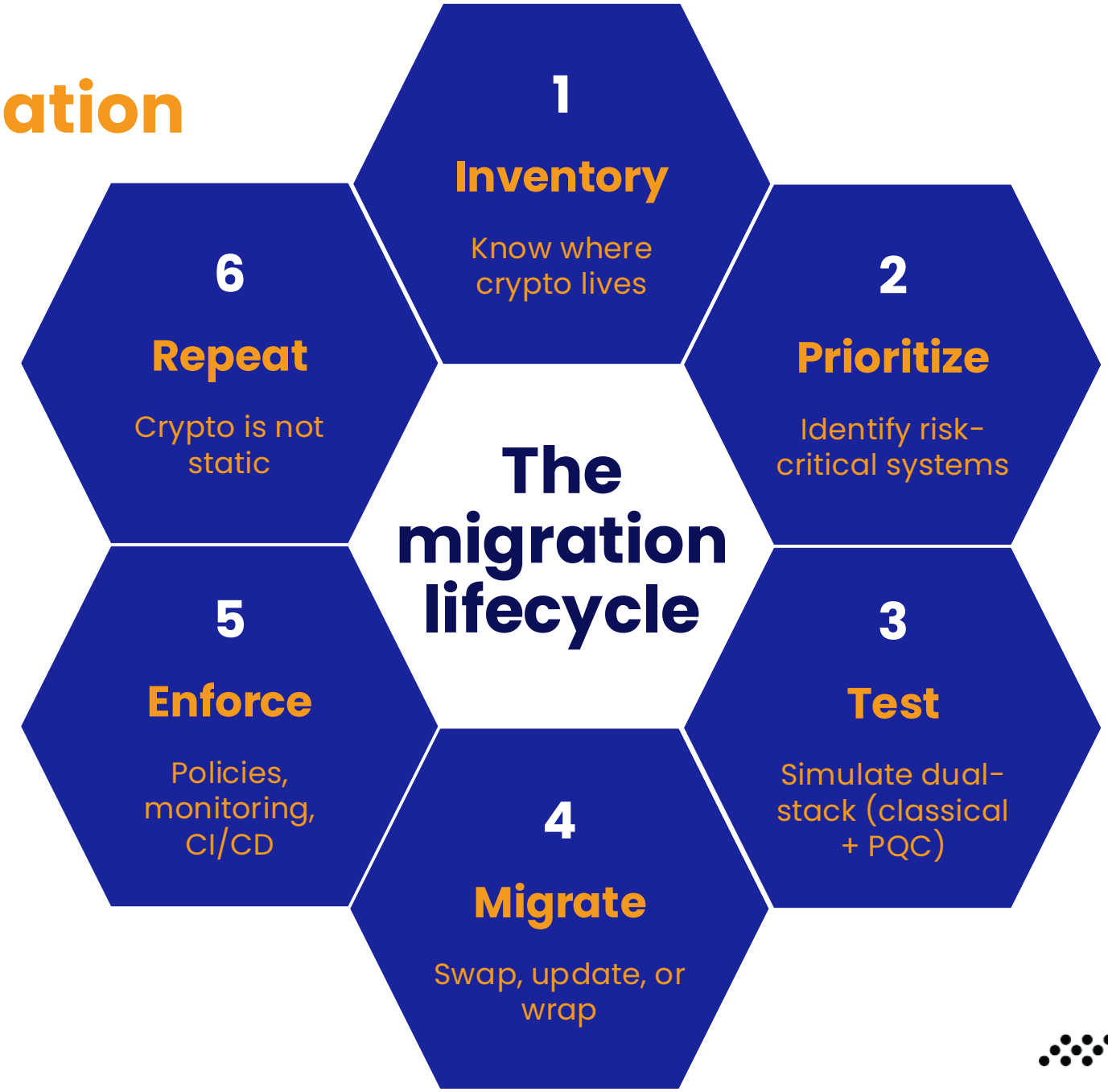
Jurisdiction	Guidance	Timeline
US (NSM-10)	a) Algorithm inventory b) Migration c) Exclusive PQC	a) 2022 and onwards b) 2025-2030 c) By 2035
US (NIST)	a) First PQC Standards b) RSA, ECC deprecated c) RSA, ECC disallowed	a) 2024 b) 2030 c) 2035
UK	a) Algorithm inventory b) Migration c) Exclusive PQC	a) By 2028 b) By 2031 c) By 2035
EU	a) National roadmaps b) EU roadmap c) Migration	a) By 2025 b) By 2027 c) By 2030

SSH

Steps for PQC migration

What are the steps to achieve Post-Quantum readiness?

PQC is not the end of the cryptographic evolution - it's not static.



SSH

SSH | Defensive Cybersecurity

Quantum-Proof Your Cybersecurity with SSH

SSH

SSH involvement in PQC development

NIST PQC Conference Panel Discussion

The White House, 2024

Singapore Govware 2022 and 2023

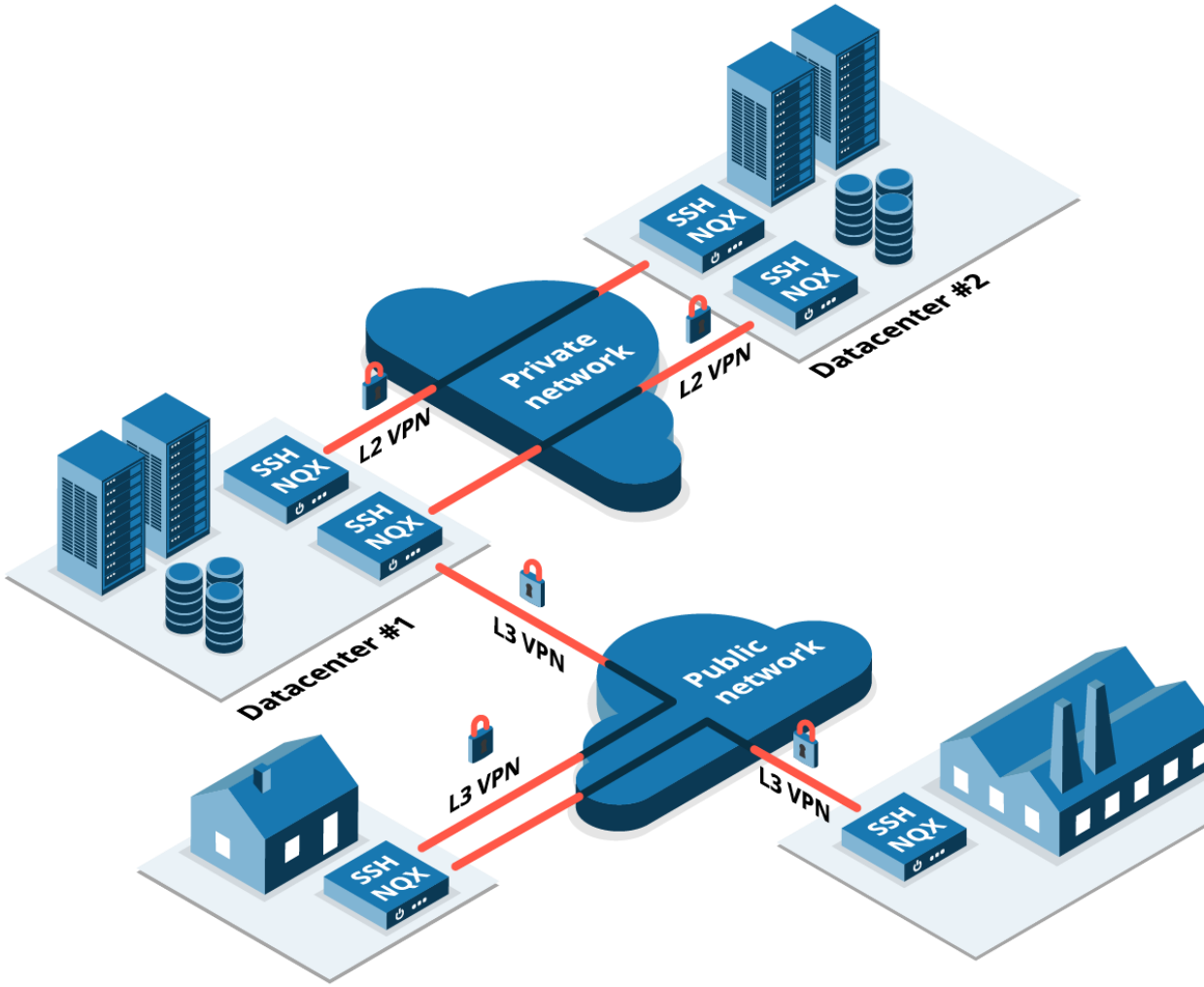
- **Suvi Lampila**
- SSH Fellow, NCCoE Consortium member

SSH

NQX securing Data-in-Transit

Protect Critical data transported over untrusted networks.

- **Connect Local networks securely over any networks** – are those public, private, service operators etc.
- **Purpose built encryption system**
  NQX inbuilt tunneling mechanisms ensure configurations meet the requirement for transporting confidential data.
- **PQC resilient as day 1**.
  Strongest encryption methods in use. PQC resilient key exchange algorithms available.



APPLIANCES

NQX 120
Remote mobile & OT

1Gbps VPN
3 x 1 Gbps
DIN rail
12 VDC
-40..+70°C

NQX 1160
Small & Medium offices

6 Gbps VPN
6 x 1 Gbps
2 x 10 Gbps SFP+

NQX 1170
medium & Large offices

15 Gbps VPN
8 x 1 Gbps
4 x 10 Gbps SFP+

Dual Power (option)

NQX 5170
Large offices & Enterprise Hubs

30 Gbps VPN
8 x 1 Gbps
4 x 10 Gbps SFP+
2 extension slots

Dual Power
Hot Swap fans
Extensions:
8 X 1G RJ45
8 x 1G SFP
4 x 10G SFP+

NQX 5200
Data Centers

60Gbps VPN
2 x 100 Gbps QSFP
4 x 10 Gbps SFP+
2 extension slots

Dual Power
Hot swap fans

Extensions:
4 x 10G SFP+
2 x 100G QSFP28

*) interfaces can operate also at 1Gbps bandwidth by utilizing SFP interface

How PrivX Key Manager fits into PQC transition

PrivX Key Manager has several features to assist in, and facilitate PQC migration within Secure Shell (SSH) products, host keys, and user keys:

- Data collection about SSH server versions and configurations, SSH keys, host keys, and their algorithms
- Reports to track the overall status of algorithms over certain hosts, host groups, applications, and whole environment
- Policies to create actionable information about non-PQC enabled assets
- Alerts about regressions in PQC readiness found in the aforementioned assets
- Large scale jobs to replace existing user keys and host keys with PQC keys without disrupting on-going processes

Creating crypto inventory

Knowing what is actually in use
Key Manager records and tracks SSH user keys, host keys and SSH product configurations in default and custom locations.

Monitoring PQC capabilities

Tracking the transition
Key Manager is able to report PQC algorithms and PQC capable products in use.

Renewing and enforcing

Large scale key upgrades
As new PQC SSH signature algorithms are standardised, Key Manager can facilitate controlled, large scaled key renewal operations.

Is your organization ready for the post-quantum era?

Get in touch to discuss how we can help you start your PQC journey today

www.ssh.com