Quantum-Resistant Security

Gina Scinta
Deputy Chief Technology Officer
Thales Trusted Cyber Technologies

Quantum computing is advancing rapidly and its impact is likely to be large—the potential computational power could render today's encryption algorithms obsolete. To address this looming threat, the White House issued a National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM 10) in this May. The NSM 10 fact sheet states that "America must start the lengthy process of updating our IT infrastructure today to protect against this quantum computing threat tomorrow."

The memo continues by stressing that, "Central to this migration effort will be an emphasis on cryptographic agility, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards." Keep in mind that even if a crypto-analytically relevant quantum computer is a decade away, bad actors can take note of potential vulnerabilities now, and exploit them later.

Attend this session to learn how to start the transition to quantum-safe cryptography. The speaker will discuss four key factors to consider when preparing for a quantum-safe encryption strategy:

- Quantum is coming – Learn why PKI based classic crypto will become obsolete
- Know your risks – Learn how long-term data is at risk to harvesting and subject to early attacks
- Focus on crypto agility – Learn what to look for in a quantum-resistant crypto solution
- Start today – Learn how to design a quantum resistant architecture