



Navigating the Shift to Post-quantum Cryptography

Secure your data by implementing
quantum resistance

By Tim Schooley and Laurie Robb

Table of Contents

Q-Day: Accelerating risks to your sensitive data	3
Preparation starts today	4
How quantum algorithms threaten encryption	5
PQC standards take shape, but evolution continues	7
Planning for a quantum-resistant future with crypto agility	8
The Trellix approach to PQC	9
Final thoughts on the shift to PQC	10
About the authors	11

The digital age is on the verge of a profound change driven by advances in quantum computing. While this will lead to many promising breakthroughs, these machines also pose a threat to the encryption that protects our data from threats.

To address these risks, organizations must understand and prepare for post-quantum computing (PQC) without delay. Let's examine the fundamentals of PQC, why it's urgent to act now, how organizations can start preparing today, and the support that Trellix experts and technology solutions can offer for your transition.

Q-Day: Accelerating risks to your sensitive data

Quantum computers use qubits that leverage quantum mechanics like superposition and entanglement to perform calculations far exceeding classical capabilities, threatening current cryptographic standards. You may have heard the term "Q-Day," which has gained attention among security professionals. Q-Day marks the day/time when a quantum computer could break today's standard encryption.

Early estimates suggested that Q-Day was a problem for the mid-2030s. It turns out that that timeline was dangerously optimistic. Rapid advancements have pushed the consensus deadline forward to sometime in the next few years.

Fiercely competitive research in quantum computing is leading to new approaches and techniques on an almost-weekly basis. Recently, it has shown that adversaries will not need the multimillion-qubit mainframes once thought necessary to break our most common algorithmic protections.

For example, adversaries no longer need to wait for a single, monolithic supercomputer to crack public-key cryptography. Threat actors can network smaller, modular quantum systems together to enable a distributed attack. This has drastically compressed the timeline for Q-Day risk. And we know that the threats have already begun.

Rapid research advancements are speeding up the approach of the looming Q-Day milestone.

Preparation starts today

To complicate things, adversaries are already engaging in “harvest now, decrypt later” (HNDL) attacks, collecting your encrypted sensitive data—such as customer PII, financial records, or intellectual property—today, to decrypt it once powerful quantum computers emerge.

Adversaries are already engaging in “harvest now, decrypt later” attacks.

While the viability of this threat depends on the long-term value of the harvested data, some of the most prized information today will retain its worth far into the future. Information that remains critical for decades, such

as national security secrets or foundational intellectual property, is at a higher risk than other data, including names, addresses, and phone numbers that might change.

Adversaries are also preparing to engage in future “trust now, forge later” (TNFL) attacks. By recording public keys and digital signatures now, they can use a quantum computer in the future to derive the private key from the public data. They can then forge what will be perceived as valid signatures to start distributing content, which could be falsified or malicious. Consumers of the data won’t be able to tell if it’s legitimate or not.

The potential for future breaches of currently secure confidential or restricted data makes the move to PQC urgent for shielding data with enduring sensitivity. It also reinforces that organizations must place a continued emphasis on current data protection programs that prevent exfiltration and monitor for potential leakage in real time.

Adversaries are actively intercepting and storing public keys and encrypted network traffic today, waiting for the day a quantum computer can derive the private keys or break the encryption to reveal the secrets inside. Organizations that handle long-term, sensitive information such as financial records, intellectual property, or healthcare data are already at risk of exposure.

¹ [TechRadar, 2025](#)

² [IBM, Cost of a Data Breach Report, 2025](#)

³ Ibid.

65%

Around two-thirds of organizations are concerned about the rise of “harvest-now, decrypt-later” attacks¹

\$4.44 million

The average global cost of a data breach in 2025, which decreased slightly from the previous year’s cost of \$4.88 million. Encryption was identified as one of the top factors that effectively mitigated the financial impact of a breach.²

\$208K

The average reduction in data breach costs by organizations that deployed encryption.³

How quantum algorithms threaten encryption

Our current, widely used asymmetric cryptography solutions, such as RSA and ECC, rely on mathematical problems, such as factoring large numbers or solving the elliptic curve discrete logarithm problem. For decades, these problems have been considered too difficult for classical computers to solve within a reasonable timeframe, forming the bedrock of our digital security.

For decades, these problems have been considered too difficult for classical computers to solve.

The emerging quantum threat landscape initially included two key challenges to the pillars of modern cryptography, one of which has since been downgraded.

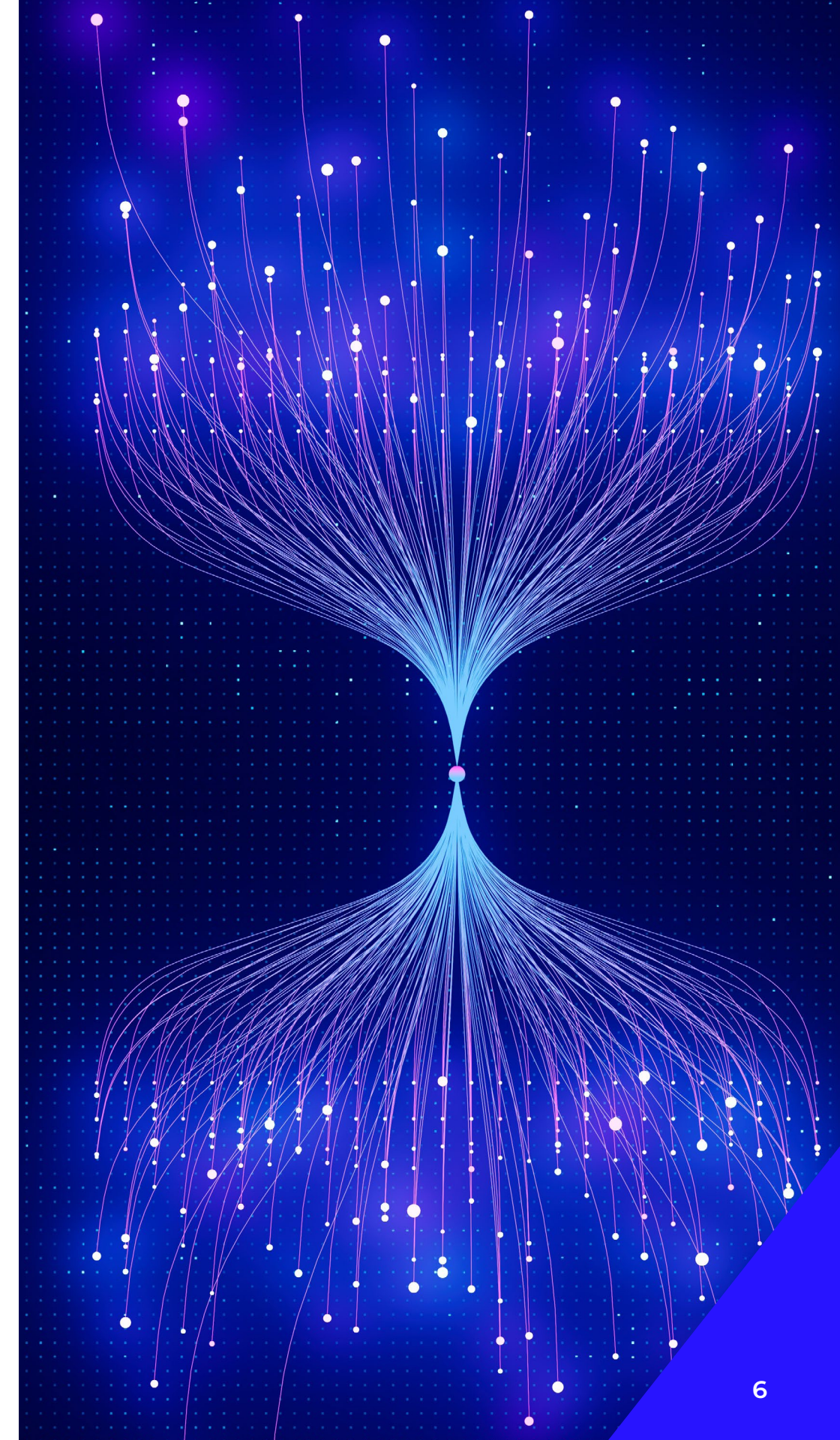
Shor's Algorithm: Shor's algorithm poses a catastrophic threat to the asymmetric (public-key) cryptography, such as RSA and ECC, that currently secures much of our digital asset infrastructure. It can efficiently solve the mathematical problems they rely on, rendering them insecure against a sufficiently powerful quantum computer.

Both RSA and ECC, despite their different mathematical underpinnings, will require replacement. This is the most immediate danger to the enterprise due to the TRFL and HNDL attack vectors we mention above.

Grover's Algorithm: While Shor's algorithm targets the specific mathematical problems underpinning asymmetric encryption, Grover's algorithm is a generic quantum search algorithm. For a long time, it was a widely accepted industry assumption that Grover's offered a massive quadratic speedup in searching through unsorted lists, effectively halving the strength of a symmetric key. Under this assumption, an AES-128 key's security would be reduced to a vulnerable 64-bit strength, prompting common recommendations to double key sizes to 256 bits to mitigate the risk.

However, leading cryptography experts and guidance from standard bodies like the U.S. National Institute of Standards and Technology (NIST) indicate this is an unlikely threat. While the potential for the quadratic speedup exists, Grover's algorithm strictly requires operations to be executed sequentially, which would be hard to operationalize in theory.

As a result, leading researchers agree that symmetric algorithms like AES-128 and SHA-256 are less of a priority. Organizations can focus their time and resources on more urgent cryptography transitions.



PQC standards take shape, but evolution continues

PQC necessitates a shift to entirely different families of mathematical problems, ones believed to be hard for both classical and quantum computers to solve. A leading approach in this new era is “lattice-based cryptography.” New standards, like CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures, incorporate this technique.

Instead of the problems that RSA and ECC use, these new algorithms derive their security from the presumed difficulty of certain complex tasks within high-dimensional geometric structures called lattices. These new mathematical foundations were chosen because they do not appear to possess the kind of structure that Shor’s algorithm can exploit, making them strong candidates for building quantum-resistant security.

NIST is leading PQC standardization. Through rigorous evaluation rounds, [NIST has selected key algorithms](#) to form the backbone of this new cryptographic era. Algorithms selected in its initial rounds include the lattice-based CRYSTALS-Kyber (ML-KEM) for key establishment and CRYSTALS-Dilithium (ML-DSA) for digital signatures, alongside the hash-based SPHINCS+ (SLH-DSA) for digital signatures as well.

Awareness of these initial standards is key for future planning. It is also important to recognize that the PQC landscape will continue to evolve, potentially with further standardization efforts or updates as research progresses and real-world deployment experience grows.

⁴ Entrust Cybersecurity Institute, 2024

⁵ DigiCert Global Study, 2023

<50%

Less than half of organizations are actively preparing for the post-quantum threat, with over one-third lacking the necessary scale or technology to transition to PQC⁴

30%

Only 30% of organizations currently allocate budget specifically for PQC readiness⁵

Planning for a quantum-resistant future with crypto agility

We anticipate a phased transition to PQC for most organizations. This methodical approach is essential for minimizing disruption and managing risk. A measured strategy also allows new PQC algorithms to gain valuable “soak time” in real-world deployments and for security organizations to gain crucial buy-in from stakeholders needed to support the transition. This time will also ensure that security professionals can identify and address unforeseen implementation issues before legacy systems are fully retired.

Key to this transition is cryptographic agility (also known as crypto agility), which is the ability to efficiently update cryptographic algorithms without significant disruptions to processes or operations. This is crucial as PQC standards mature.

It is vital to recognize that PQC is not a simple 1:1 drop-in replacement. Implementing this capability involves more than just swapping algorithms; systems must be agile enough to handle significantly larger key sizes and signature payloads. This may require more significant architectural changes to network protocols and storage. The transition starts with a thorough cryptographic inventory and strategic research to understand the landscape of vulnerable algorithms and the most effective transition to adequate protection.

Agility also means your key management systems (KMS) will need to support new PQC key types, and protocols must integrate new PQC cipher suites. Ensuring compatibility with hardware, such as smartcards, will also be expected. Since PQC is still developing, agility provides an insurance policy against future threats and allows you to adopt the best-performing PQC algorithms as needs evolve.

Organizations can take necessary steps now, including designing systems with cryptographic abstraction layers and collaborating with encryption vendors on their PQC roadmaps. They also need to allocate a specific budget for PQC readiness. Additional steps include establishing new acquisition policies concerning PQC and scheduling workforce education and training about the upcoming transition.

It is vital to recognize that PQC is not a simple 1:1 drop-in replacement.

The Trellix approach to PQC

Trellix's data encryption team embarked on an in-depth inventory of our applied cryptography in mid-2023. This foundational work evolved into an exciting collaboration with [wolfSSL](#) to integrate cutting-edge PQC into our [data encryption product line](#), including both our Drive Encryption and File & Removable Media Protection products.

Renowned for its lightweight, portable, and high-performance cryptographic library, wolfSSL offers broad support for emerging PQC algorithms. Together, Trellix and wolfSSL are actively working toward validation for [FIPS 140-3](#) for wolfSSL's cryptographic module, specifically for the Unified Extensible Firmware Interface (UEFI) environment.

Together, Trellix and wolfSSL are actively working toward FIPS 140-3 validation.

FIPS is one of the most widely accepted standards for cryptography compliance, especially in the public sector, supply chain, and other regulated industries. Through this initiative, we plan to bring robust, certified PQC security to the foundation of [Trellix Drive Encryption](#), where authentication occurs at the time of system boot.

We also plan to phase out legacy asymmetric cryptography vulnerable to quantum attacks in Trellix solutions. To ensure our data encryption products are fully prepared for the post-quantum future, Trellix is working to achieve a new level of crypto agility by:

- Discontinuing noncompliant algorithms
- Integrating the Wolf SSL module into our products
- Transitioning algorithms over-the-air without system reboots or a full drive decryption
- Creating dedicated programs to facilitate smooth customer transitions

Our objective is a fully quantum-resistant security posture. Customers can count on us for ongoing vigilance and to adapt to new standards as needed.



Final thoughts on the shift to PQC

The shift to post-quantum cryptography is a significant undertaking and a necessary one. Trellix experts are ready to guide customers through this transition by identifying their most critical data, assessing cryptographic dependencies, and strategically integrating PQC solutions into existing infrastructure—helping to ensure their most sensitive data remains secure against today's threats and the quantum challenges of tomorrow.

[Contact us](#) for more information on [Trellix Data Encryption](#) or to be connected with one of our Professional Services experts to begin planning for your transition to a quantum-resistant future.

About the authors



Tim Schooley
Senior Product Manager
Trellix Data Security

Tim Schooley has dedicated his entire 18-year career to the mission of keeping customer data safe, consistently contributing to and driving innovation within the Trellix Data Security portfolio. With a background in computer science, he leverages his deep knowledge of building secure systems to guide product evolution as a Senior Product Manager. He navigates the complexities of modern cryptography, like post-quantum standards, and adapts to dynamic regulatory environments. Tim frequently bridges the technical and business realms, ensuring solutions are both forward-looking and grounded in real-world operational requirements.



Laurie Robb
Senior Director
Product Management for Data Security

Laurie has more than 25 years of experience spanning cybersecurity, SaaS, technology, and corporate leadership. As Senior Director, Product Management for Data Security at Trellix, she leads the strategy and evolution of data security solutions that help organizations protect critical enterprise data while addressing emerging challenges, including those associated with AI adoption. Drawing on a background in both product management and product marketing, Laurie brings a strong customer and partner perspective to the delivery of innovative security capabilities that drive business outcomes. She is passionate about solving complex security challenges and translating customer needs into impactful solutions. Laurie is also a member of the leadership team for Women in Cybersecurity, Northeast Ohio Affiliate.



Trellix is a global cybersecurity company delivering intelligence-led cyber resilience for security-conscious organizations at any stage of their journey. Transforming over 30 years of threat intelligence into high-fidelity detections and automating AI-driven detection and response across cloud, on-premises, air-gapped, and operational technology environments, Trellix helps customers adapt to the constantly evolving threat landscape.

More at trellix.com

Follow Trellix on [LinkedIn](#) and [X](#).