

2026 Global Quantum Security Intelligence Report

Trends, Timelines, Crypto-Agility, Getting Started



Why 2026 Is the Year of Quantum Security

Your bank's encrypted data from 2024 already sits on cybercriminals' hard drives and is waiting to be decrypted when the quantum computer becomes mainstream. With the QuantWare 10,000-qubit processor announced, decades of "secure" data will crack open. This "harvest now, decrypt later" attack has been occurring for the last few years, and it's now accelerating.

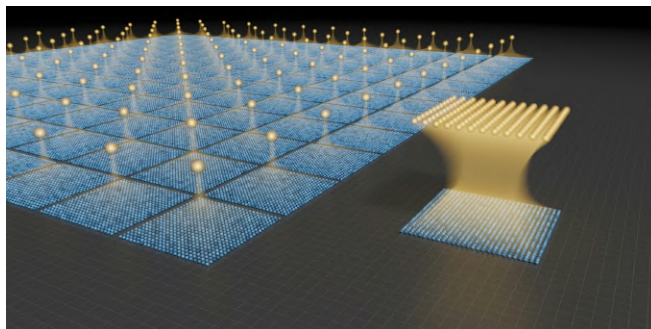
RESEARCH PAPER

How fast is "decrypt later" accelerating?

John Preskill, Cal Tech's Richard P. Feynman Professor of Theoretical Physics, states, "I've been working on fault-tolerant quantum computing longer than some of my coauthors have been alive. Now at last we're getting close." Their new March 2026 research points to a shocking 100x efficiency breakthrough:

Earlier the same week that the Cal Tech research was published, Google publishes, "We're setting a timeline for post-quantum cryptography migration to 2029."

Google's Sophie Schmieg, Senior Staff Cryptography Engineer, and Heather Adkins, VP, Security Engineering, said, "This new timeline reflects migration needs for the PQC era in light of progress on quantum computing hardware development, quantum error correction, and quantum factoring resource estimates."



"Useful Quantum Computers Could Be Built with as Few as 10,000 Qubits"
March 31, 2026 California Institute of Technology research paper.



"Quantum frontiers may be closer than they appear" - March 25, 2026 Google

2026 marks the shift from quantum awareness to action. Following 2025's International Year of Quantum Science and Technology, governments now enforce hard deadlines. The quantum computing market hit \$2 billion (Investing.com, 2026), while post-quantum cryptography races from \$420 million (2025) to \$2.84 billion by 2030 (Market Research, 2026). Organizations have 3-5 years to overhaul encryption.

Hence, the message is very clear.

Quantum security isn't tomorrow's problem.

It's today's mandate.

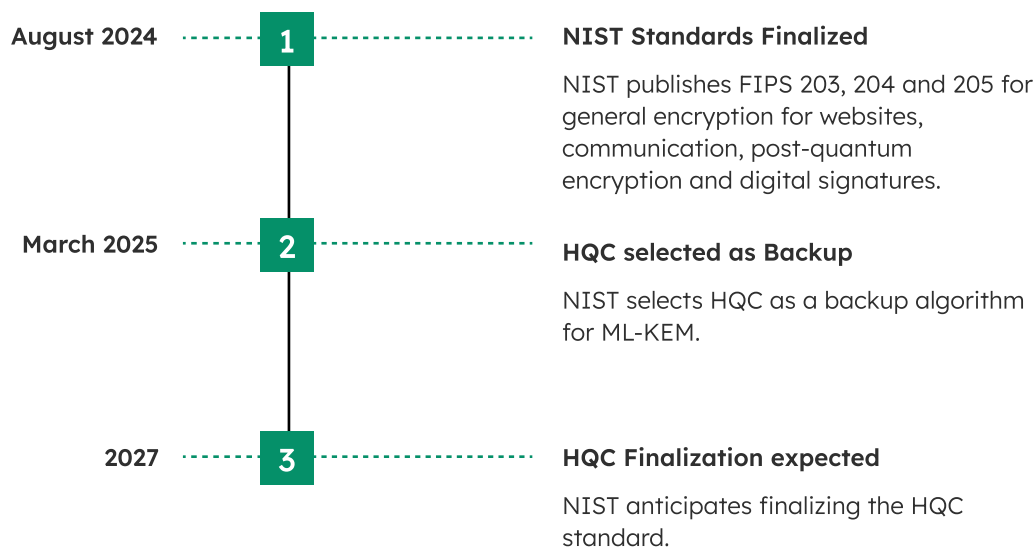
This Quantum Security Intelligence Report details 10 critical trends shaping 2026, & the actions to take now.

The 10 Quantum Cybersecurity Trends Defining 2026

TREND 1

Post-Quantum Cryptography Migration Mandates

Governments worldwide are no longer suggesting quantum-safe transitions, they're demanding them.



(NIST Standards Published) In August 2024, the U.S. National Institute of Standards and Technology finalized critical post-quantum cryptography standards (NIST, 2024):

1. FIPS 203 (ML-KEM)

General encryption for websites, communications

2. FIPS 204 (ML-DSA)

Digital signatures for authentication

3. FIPS 205 (SLH-DSA)

Hash-based signatures as backup

4. FIPS 206 (FALCON)

High-performance signatures

5. HQC (Hamming Quasi-Cyclic)

Backup algorithm for ML-KEM

What This Means

Every organization using RSA, ECC, or other vulnerable encryption must migrate to these standards. The process takes 3-5 years, so starting in 2026 means finishing around 2030-31.

TREND 2

Harvest Now, Decrypt Later (HNDL) Defense Becomes Urgent

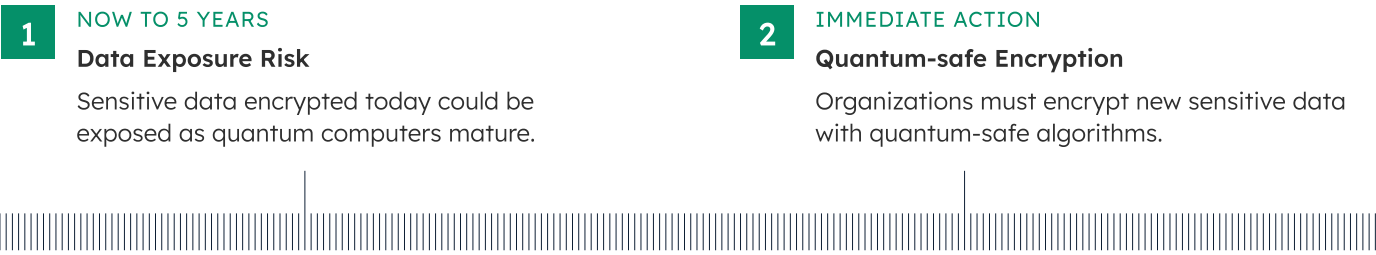
Adversaries aren't waiting for quantum computers, they're stealing encrypted data today to decrypt tomorrow.

Security experts warn that sensitive data encrypted now could be exposed anytime between now to next 5 years as quantum computers mature. This particularly threatens:

- Healthcare records (50+ year retention requirements)
- Financial transactions and trading algorithms
- Government classified communications
- Pharmaceutical research worth billions
- Long-term business contracts and IP

Defense Strategy

Organizations must immediately encrypt new sensitive data with quantum-safe algorithms, even if full migration takes years.



Quantum Security Threats and Defense Strategy

TREND 3

Crypto-Agility Becomes Essential Architecture

Crypto-agility means systems that can rapidly swap encryption algorithms without major disruption. Future encryption upgrades and enhancements are seamless and painless.

Why it matters -

- New vulnerabilities in PQC algorithms may be discovered
- Standards will evolve based on real-world testing
- Sovereign algorithm requirements are already appearing in government policy documents and RFPs (Request for Proposals)
- Organizations need flexibility to respond to new threats quickly

Implementation

Abstract cryptographic functions from business logic, implement cryptographic service layers, and maintain algorithm versioning systems.

TREND 4

Quantum Key Distribution (QKD) Global Market Explodes

The QKD market is projected to reach \$1.61 billion in 2026, with satellite-based and photonic chip systems enabling secure global networks. The QKD Market will grow to \$19.47 Billion in 2035 with 31.6% CAGR (Source: Various Research Houses – Research & Markets and others).

Growth Drivers -

1. Satellite-based QKD

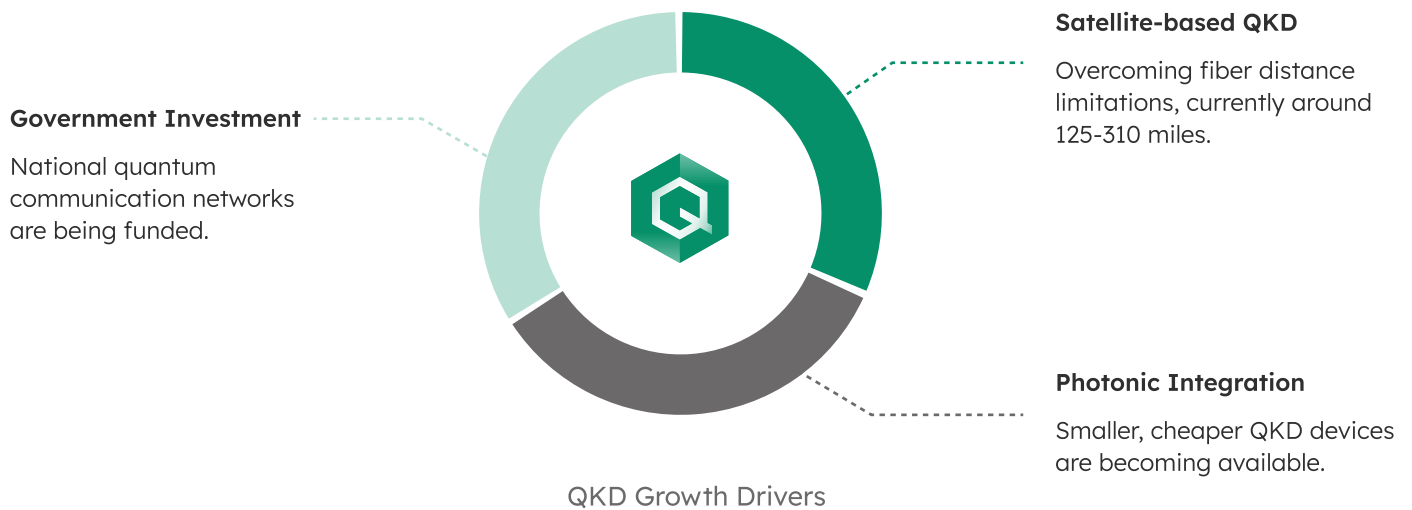
Overcoming fiber distance limitations (currently ~125-310 miles)

2. Photonic integration

Smaller, cheaper QKD devices

3. Government investment

National quantum communication networks



Regional Leadership -

1. North America

34% market share, led by U.S. government mandates

2. Asia-Pacific

Fastest growth at 19.7% CAGR, driven by China, India, Singapore

3. Europe

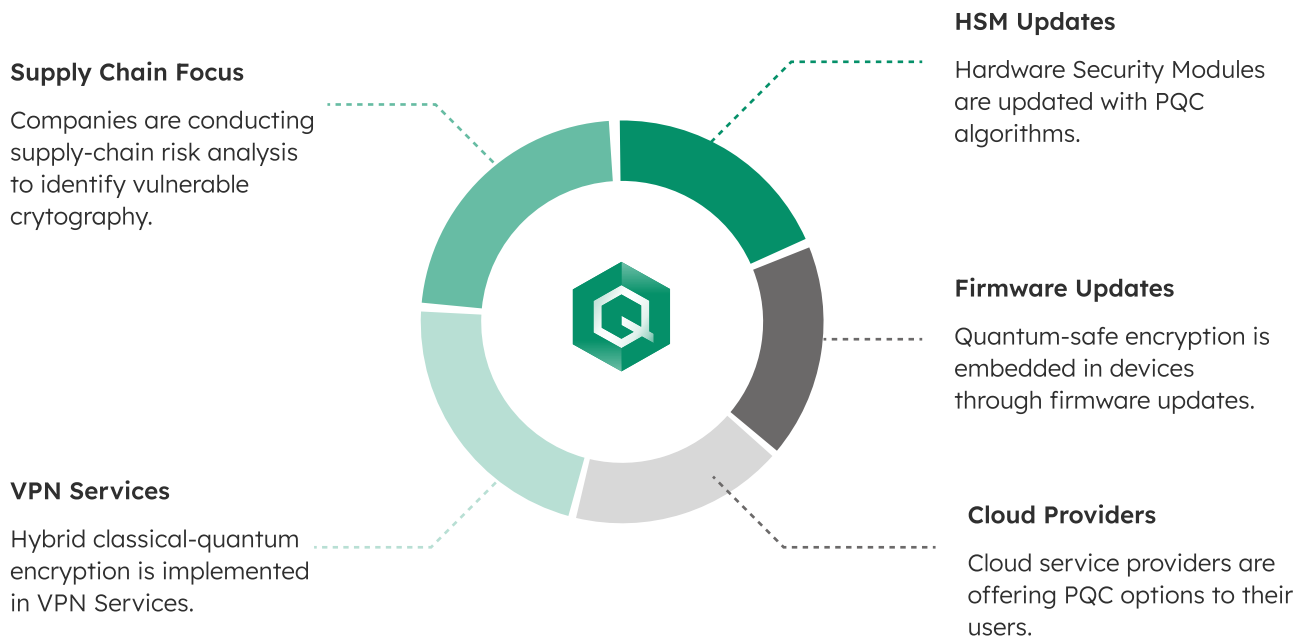
Strong adoption through EuroQCI initiative

Key Application Sectors

Banking, government, defense, healthcare, telecommunications.

TREND 5

Quantum-Resistant Hardware and Software Integration



Organizations are integrating quantum-resistant solutions into legacy systems through:

1. Hardware Security Modules (HSMs)

Updated with PQC algorithms

2. Firmware updates

Embedding quantum-safe encryption in devices

3. Cloud service providers

Offering PQC options (AWS, Microsoft Azure, Google Cloud)

4. VPN services

Implementing hybrid classical-quantum encryption

Supply Chain Focus

Companies are conducting supply-chain risk analysis to identify where vulnerable cryptography exists in third-party software and hardware.

TREND 6

Regulatory Roadmaps and Compliance Deadlines

Countries worldwide are establishing quantum security mandates -

1. European Union

The EU Post-Quantum Cryptography Roadmap requires high-risk sectors (finance, healthcare, critical infrastructure) to begin transitions by end of 2026 (Telefonica, 2026). Full migration expected by 2030-2035.

2. United States

Federal agencies must inventory cryptographic systems and begin PQC migration under National Security Memorandum guidance (NIST, 2024).

3. United Kingdom

NCSC (National Cyber Security Centre) published detailed guidance for quantum-readiness, emphasizing cryptographic inventories and phased replacements.

4. Singapore

Launched the National Quantum-Safe Network (NQSNI) initiative, partnering with industry to deploy quantum-secure communications infrastructure.

5. Middle East

UAE and Saudi Arabia investing heavily in quantum technologies as part of digital transformation strategies, with cybersecurity as priority area.

6. China

Operational national quantum communication backbone, mandating quantum security for critical government and financial sectors.

TREND 7

Market Growth Signals Strategic Importance

The numbers reveal quantum security's strategic priority -

1. Quantum computing market

\$2 billion in 2026, growing exponentially (Investing.com, 2026)

2. Post-quantum cryptography market

From \$420 million (2025) to \$2.84 billion (2030)

3. Quantum cryptography market

\$820 million in 2026, reaching \$3.73 billion by 2035 at 18.3% CAGR (Roots Analysis, 2025)

4. Defense sector leadership

Military and intelligence agencies driving quantum computing investment

Investment Focus Areas

QKD hardware, PQC software solutions, consulting services (45% of market), quantum-safe network infrastructure.

TREND 8

AI and Quantum Threat Synergies

**AI Enhancing Quantum Attacks**

Agentic AI accelerates cryptographic vulnerability discovery, optimizes quantum algorithms for code-breaking, and enables automated exploitation at machine speed.

**AI Defending Against Quantum Threats**

Predictive models forecast quantum computing timelines, AI-powered crypto-agility systems enable rapid algorithm updates, automate PQC migration planning, and provide real-time threat intelligence on quantum attack development.

TREND 9

Global Co-ordination Through "Year of Quantum Security"

The Year 2025 - International Year of Quantum Science and Technology achieved its goal, moving quantum from specialist circles into mainstream strategy discussions. Now, in 2026, the focus shifts from quantum awareness to quantum security implementation, recognizing that protection determines deployment success.

2026 has been designated the "Year of Quantum Security" by industry leaders, emphasizing international cooperation (The Quantum Insider, 2026):

- Global standards alignment (ISO, NIST, ETSI coordination)
- Intellectual property protection frameworks for quantum tech
- Public-private partnerships for quantum infrastructure
- International threat intelligence sharing
- Cross-border quantum communication networks



Major Conferences to participate

World Economic Forum, RSA Conference, and quantum-specific summits driving policy coordination.

TREND 10

Skills Gap and Workforce Development Crisis

With only 30,000 quantum professionals globally (Source: TieTalent) and a 3:1 job-to-candidate ratio (Source: McKinsey), the quantum workforce shortage has become critical.

Training Focus Areas:

- Post-quantum cryptography implementation
- QKD network engineering
- Quantum risk assessment
- Crypto-agility architecture
- DevSecOps with quantum security integration

Solutions Emerging:

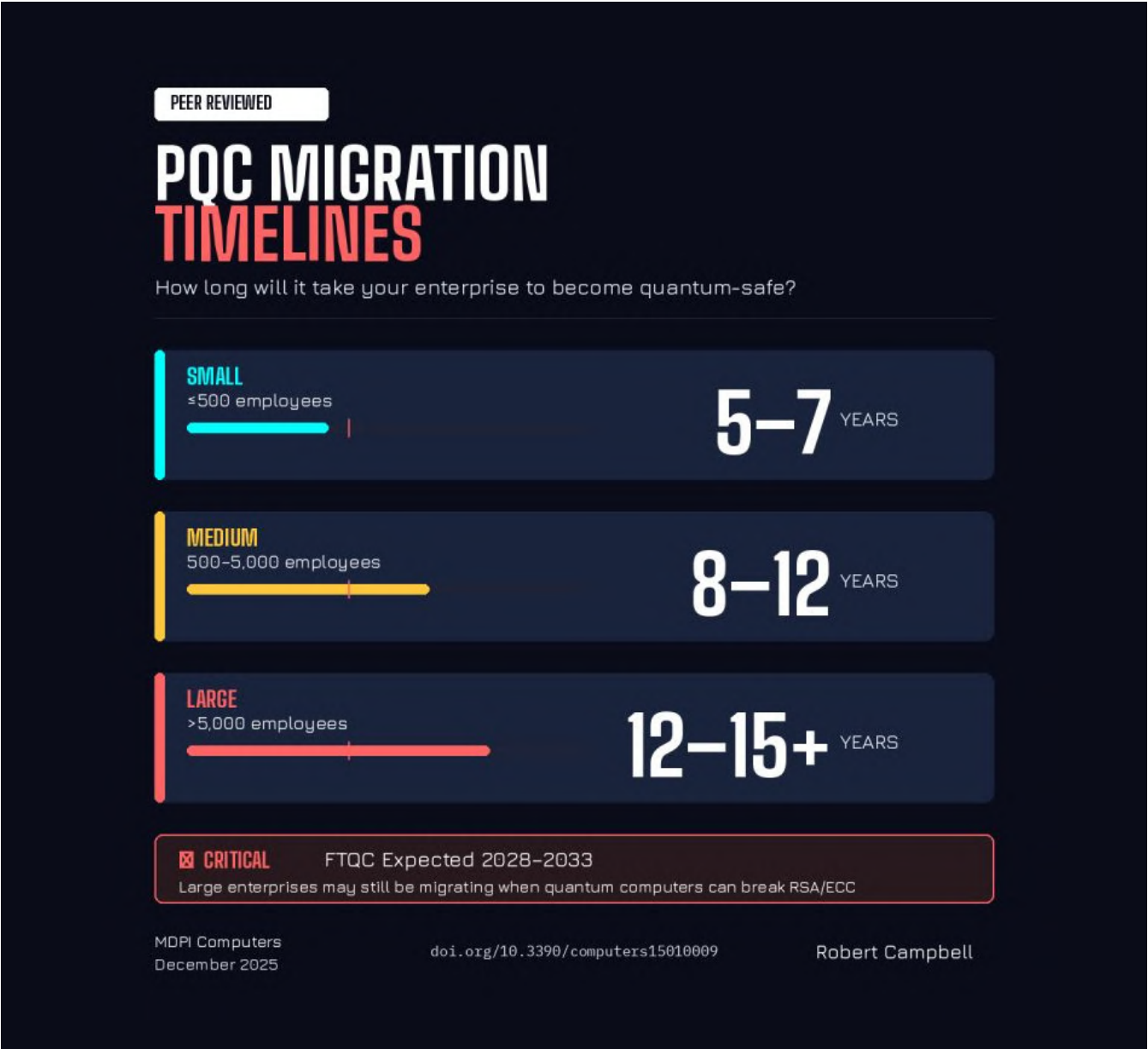
- University quantum security programs
- Professional certification courses
- Corporate training partnerships
- Hands-on lab environments
- Vendor-provided education

TREND ACCELERATOR

PQC Migration Timelines

Dr. Robert Campbell, FBBA

Independent Researcher, Upper Marlboro, MD 20774, USA
IBM Quantum-Safe Executive | Quantum-Era AI Security Researcher | IBM DoD PQC Migration Curriculum Developer |
Ph.D. Quantum Resistant Cryptography | Fellow, British Blockchain Association | IBM Quantum Ambassador



Source Report: [Enterprise Migration to Post-Quantum Cryptography: Timeline Analysis and Strategic Frameworks](#)

The transition to Post-Quantum Cryptography (PQC) represents a watershed moment in the history of our digital civilization. Organizations planning for a 3-5 year "upgrade" will fail. The reality is a 10-15-year systemic transformation.

Novel Framework Analysis

Causal dependency mapping (HSM certification, partner coordination as critical paths)

- "Zombie algorithm" maintenance overhead quantified (20-40%)
- Zero Trust Architecture implications for PQC



Practical Guidance

Crypto-agility frameworks and phased migration strategies for immediate action.

Strategic Recommendations for Leadership:

1. Prioritize by Data Value, Not System Criticality

Invert the traditional triage model. Systems protecting long-lived data (IP, PII, Secrets) must migrate first, regardless of their operational uptime criticality, to mitigate SNDL.

2. Fund the "Invisible" Infrastructure

Budget immediately for the expansion of PKI repositories, bandwidth upgrades, and HSM replacements. These are long-lead items that cannot be rushed.

3. Establish a Crypto-Competency Center

Do not rely solely on generalist security staff. Invest in specialized training or retain dedicated PQC counsel to navigate the mathematical and implementation nuances. The talent shortage will only worsen.

4. Demand Vendor Roadmaps

Contractual language must shift. Procurement should require vendors to provide binding roadmaps for PQC support. "We are working on it" is no longer an acceptable answer for critical supply chain partners.

5. Embrace Hybridity

Accept that the future is hybrid. Design architectures that can support dual-stack cryptography indefinitely, viewing it not as a temporary bridge but as a long-term operational state.

6. Implement Automated Discovery

You cannot migrate what you cannot see. Deploy automated cryptographic discovery tools to continuously map the cryptographic posture of the estate, identifying shadow IT and legacy instances that manual surveys miss.

How Organizations Should Prepare for Quantum Threats

STEP 1

Cryptographic Inventory & Quantum-safe Blueprint Engagement (1H 2026)

STEP 2

Finalize Detailed Migration Roadmap, Begin Deployment (2H 2026)

Engage expert consultants, inventory all cryptographic assets, prioritize highest-risk systems, select appropriate PQC algorithms, plan a hybrid encryption strategy, budget for 3-7 year migration.

STEP 3

Begin Implementation (Q3-Q4 2026)

Deploy PQC for new sensitive data, pilot QKD for critical communications, train security and IT teams, update policies, and test quantum-safe solutions in production.

STEP 4

Maintain Continuous Improvement (Ongoing)

Monitor quantum computing progress, update algorithms as standards evolve, conduct regular security audits, and stay engaged with industry quantum communities.

The Bottom Line

2026 is Your Deadline

Quantum computers capable of breaking encryption arrived in 2025 and will become mainstream by 2028-2035. Enterprises need 3-5 years to migrate systems, start in 2026, finish by 2029-2030.

Global consensus is clear: EU mandates, NIST standards, and explosive market growth demand immediate action. Leading nations (USA, China, EU, Singapore, India, Middle East, UK) are establishing competitive advantages through quantum-safe infrastructure now.

“The question isn’t whether quantum computers will break encryption, it’s whether your organization will be protected when they do.”

Your Next Steps?

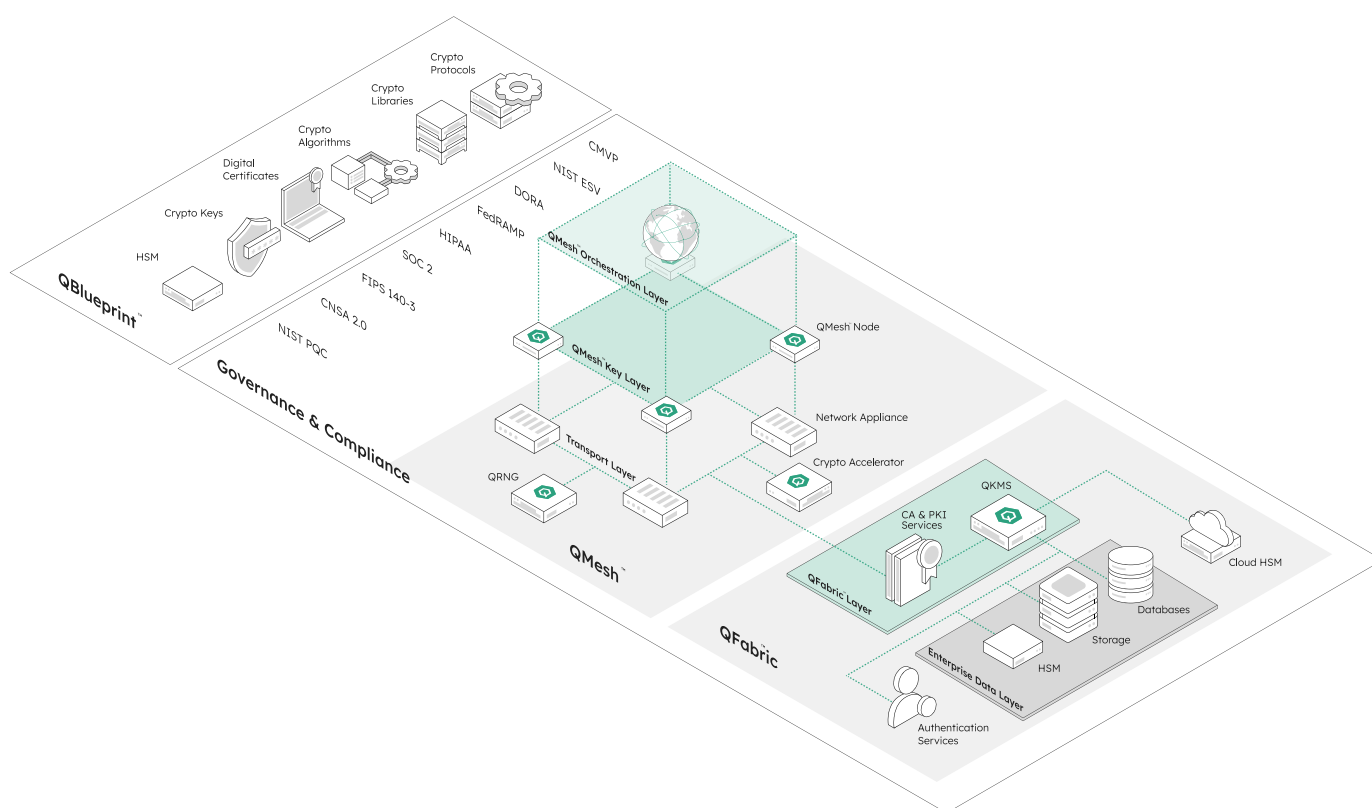
Cryptographic Inventory, Risk Prioritization & Compliance Alignment, Quantum-safe Blueprint. Develop your customized migration roadmap, and partner with proven experts like enQase to secure your communication and data’s future across all layers: from hardware to services, network to edge, platform to infrastructure

Advantages of the Full Stack, Quantum Encryption Solutions Company

enQase is the only USA-based, full-stack quantum-safe security platform that unifies proven cryptography, quantum hardware grounded in physics, and a powerful integration layer to deliver comprehensive protection and crypto-agility for the quantum era.

The enQase Platform empowers enterprises, defense organizations, cloud providers, and critical infrastructure operators to seamlessly adopt quantum-safe technologies while achieving crypto agility across their ecosystems. By combining quantum-grade hardware with software defined control and interoperability, enQase ensures alignment with NIST standards, delivers unmatched flexibility and compliance readiness, and reduces risk across data, network, and compute layers, all while maintaining business continuity and operational resilience in an evolving cryptographic landscape.

The enQase Quantum Safe Platform





www.enqase.com