

# The Global Post-Quantum Cryptography Market 2026–2036

<https://marketpublishers.com/r/G3728B901453EN.html>

Date: May 2026

Pages: 130

Price: US\$ 1,400.00 (Single User License)

ID: G3728B901453EN

## Abstracts

Post-quantum cryptography (PQC) addresses the most consequential security transition in a generation: the replacement of public-key cryptography that a sufficiently powerful quantum computer would render obsolete. The algorithms securing virtually all digital communication today — RSA, elliptic-curve cryptography, and Diffie-Hellman key exchange — rest on mathematical problems that Shor's algorithm, running on a cryptographically relevant quantum computer (CRQC), can solve efficiently. The arrival of such a machine, termed "Q-Day," is estimated by most observers to fall between 2030 and 2040, though with considerable uncertainty. PQC algorithms are designed to resist both classical and quantum attack while running on conventional hardware, which makes broad, software-driven migration possible.

The market reached an inflection point with the conclusion of the US National Institute of Standards and Technology (NIST) standardization process, which finalized ML-KEM, ML-DSA, and SLH-DSA as Federal Information Processing Standards in 2024. Standardization converted PQC from a research field into a procurable, mandatable technology and gave governments and regulated industries a concrete migration target.

A defining feature of the market is that the algorithms themselves are a small economic prize, while the migration to them is a very large one. The NIST standards compile to a few hundred kilobytes of code; deploying them across decades of accumulated cryptographic infrastructure — protocols, applications, hardware security modules, certificate hierarchies, firmware, and supply chains — is an enterprise-wide undertaking. Migration framework documents from NSA, NIST, ENISA, and major consultancies converge on a consistent estimate: services and integration spending will exceed underlying PQC product revenue by a factor of roughly 8–12? across the migration window.

Demand is driven by NIST standardization, government migration mandates such as NSA CNSA 2.0, the harvest-now-decrypt-later threat to long-lived data, sector regulation in finance, telecommunications and critical infrastructure, and the structural need for crypto-agility. The principal restraints are organizational inertia, backward-compatibility concerns arising from larger post-quantum key sizes, scarce specialist talent, and uncertainty over Q-Day's exact timing.

Banking and defence anchor near-term demand; embedded and IoT migration grows fastest later in the forecast. North America leads the market, supported by the earliest and most prescriptive mandates, with Europe and Asia-Pacific following. The total addressable market — products plus migration services — is projected to expand from a few billion dollars in 2026 to several tens of billions by 2036, making PQC one of the defining cybersecurity markets of the coming decade.

The *Global Post-Quantum Cryptography Market 2026–2036* examines the post-quantum cryptography opportunity across products, services, technologies, end-use industries, and regions over a ten-year horizon. As quantum computing advances toward the point at which it can break the public-key cryptography securing modern digital communication, organizations worldwide face an urgent and complex migration. This report quantifies that opportunity and provides the strategic analysis needed by vendors, investors, integrators, and security leaders.

The report opens by establishing the quantum threat — Shor's and Grover's algorithms, the concept of a cryptographically relevant quantum computer, the Q-Day timeline, and the harvest-now-decrypt-later attack model that makes migration urgent regardless of when Q-Day arrives. It examines the four families of post-quantum cryptography — lattice-based, hash-based, code-based, and multivariate — and the NIST-standardized algorithms ML-KEM, ML-DSA, SLH-DSA, and FN-DSA, including the practical consequences of their larger key and signature sizes.

A detailed treatment of the standards and regulatory landscape covers the NIST process, the FIPS standards, NSA CNSA 2.0, the IETF, ETSI, ISO/IEC and ITU bodies, and national guidance from ENISA, BSI, NCSC, and ANSSI. The report then analyses the quantum-safe migration stack layer by layer — cryptographic discovery, crypto-agility, hybrid cryptography, HSMs, quantum-safe TLS and PKI, code signing, and embedded systems — and the central finding that migration services outweigh product revenue by 8–12%.

The report provides extensive market analysis: drivers and restraints, SWOT analysis, a technology-readiness assessment, an opportunity-assessment framework, and per-segment SWOTs. It develops industry-specific migration programmes for banking, defence, government, telecommunications, critical infrastructure, cloud, healthcare, and automotive/IoT/manufacturing, and analyses the migration-services market and its provider landscape. Granular ten-year forecasts (2026–2036) are provided for the total addressable market and segmented by cryptographic approach, product category, end-user group, and region, with conservative, base, and optimistic scenarios. A regional analysis covers North America, Europe, Asia-Pacific, and the Rest of World.

The report includes profiles of 42 key companies active in post-quantum cryptography, covering their country, business description, funding, and PQC products and technology. Supported throughout by data tables and figures, the report is an essential strategic resource for any organization seeking to understand, enter, or invest in the post-quantum cryptography market.

**Contents include:**

Quantum threat, NIST outcomes, why migration is the market, headline forecast, drivers and restraints, regional summary, principal findings

What PQC is, classical public-key vulnerabilities, Shor's and Grover's algorithms, symmetric vs. public-key cryptography, PQC vs. QKD vs. QRNG, terminology, scope and methodology

The Quantum Threat and Q-Day Timeline — cryptographically relevant quantum computers, harvest-now-decrypt-later, Q-Day estimates, long-lived data risk, hardware roadmaps, strategic implications

PQC Algorithms and Technology — lattice-based, hash-based, code-based, multivariate and isogeny-based cryptography, performance comparison, NIST Round 4, key and signature size implications

Standards and the Regulatory Landscape — NIST process, FIPS 203/204/205/206, NSA CNSA 2.0, IETF/ETSI/ISO/ITU, national guidance, sector regulators

The Quantum-Safe Migration Stack — cryptographic discovery, crypto-agility, hybrid cryptography, HSMs, quantum-safe TLS/IPsec/VPN/SSH, PKI, code

signing, embedded and IoT

PQC Products and Delivery Models — cryptographic libraries, software and firmware, PQC-enabled browsers, chips and accelerators, HSMs and tape drives, cloud/VPN/PQCaaS, product market structure

Market Analysis and Opportunity Assessment — drivers, restraints, net impact, SWOT, services-to-product ratio, technology readiness, opportunity framework, end-use opportunities, per-segment SWOTs

Industry-Specific Migration Programs — banking, defence, government, telecommunications, critical infrastructure, cloud and SaaS, healthcare, automotive/IoT/manufacturing, comparative summary

Migration Services and Consulting — market structure, pure-play consultancies, systems integrators, cloud-vendor services, specialty hardware vendors, managed services, strategic implications

Market Forecasts 2026–2036 — total addressable market, forecasts by cryptographic approach, product category, end-user group, and region, migration services forecast, growth scenarios

Regional Analysis — North America, Europe, Asia-Pacific, Rest of World, regional forecast and share dynamics

Company Profiles — 42 company profiles

The report profiles the following 42 companies active in the post-quantum cryptography market: 01 Quantum Inc., Aires Applied Quantum Technology (AAT), Atos, BTQ Technologies, China Telecom Quantum Group, Cisco Systems, Cloudflare, Crypto4A Technologies, Crypto Quantique, CryptoNext Security, DigiCert, Entrust, evolutionQ, Google, IBM, Infineon Technologies, Intel, ISARA, KETS Quantum Security, Microsoft, Patero, Post-Quantum (PQ Solutions), PQSecure Technologies, PQShield, Project Eleven, QAN Platform, QuantiCor Security, Quantropi, Quantum Secure Encryption Corp. (QSE), QuBalt and more...

## Contents

### **1 EXECUTIVE SUMMARY**

- 1.1 The Quantum Threat in Brief
- 1.2 NIST Standardization Outcomes
- 1.3 Why Migration Is the Market
- 1.4 Headline Market Forecast
- 1.5 Drivers and Restraints
- 1.6 Regional Summary
- 1.7 Principal Findings and Strategic Recommendations

### **2 INTRODUCTION**

- 2.1 What Is Post-Quantum Cryptography?
- 2.2 Classical Public-Key Cryptography and Its Vulnerabilities
- 2.3 Shor's and Grover's Algorithms
- 2.4 Symmetric vs. Public-Key Cryptography in a Quantum World
- 2.5 PQC vs. QKD vs. QRNG
- 2.6 Cryptographic Terminology
- 2.7 Report Scope, Segmentation, and Methodology

### **3 THE QUANTUM THREAT AND Q-DAY TIMELINE**

- 3.1 Cryptographically Relevant Quantum Computers
- 3.2 The Harvest-Now-Decrypt-Later Model
- 3.3 Q-Day Estimates and Uncertainty
- 3.4 Long-Lived Data and Retention Risk
- 3.5 Quantum Hardware Roadmaps
- 3.6 Strategic Implications

### **4 PQC ALGORITHMS AND TECHNOLOGY**

- 4.1 Lattice-Based Cryptography
- 4.2 Hash-Based Cryptography
- 4.3 Code-Based Cryptography
- 4.4 Multivariate and Isogeny-Based Cryptography
- 4.5 Algorithm Performance Comparison
- 4.6 NIST Round 4 and Signature Diversity

#### 4.7 Key and Signature Size Implications

### **5 STANDARDS AND THE REGULATORY LANDSCAPE**

#### 5.1 NIST Standardization Process

#### 5.2 The FIPS 203/204/205/206 Standards

#### 5.3 NSA CNSA 2.0

#### 5.4 IETF, ETSI, ISO/IEC, ITU

#### 5.5 National Guidance (ENISA, BSI, NCSC, ANSSI)

#### 5.6 Sector Regulators

### **6 THE QUANTUM-SAFE MIGRATION STACK**

#### 6.1 Cryptographic Inventory and Discovery

#### 6.2 Crypto-Agility Frameworks

#### 6.3 Hybrid Cryptography

#### 6.4 HSMs with PQC

#### 6.5 Quantum-Safe TLS, IPsec, VPN, and SSH

#### 6.6 Quantum-Safe PKI

#### 6.7 Quantum-Safe Code Signing

#### 6.8 Embedded Systems and IoT

### **7 PQC PRODUCTS AND DELIVERY MODELS**

#### 7.1 Cryptographic Libraries

#### 7.2 PQC Software and Firmware

#### 7.3 PQC-Enabled Browsers

#### 7.4 PQC Chips and Hardware Accelerators

#### 7.5 PQC-Enabled HSMs and Tape Drives

#### 7.6 PQC Cloud, VPN, and PQC-as-a-Service

#### 7.7 Product Market Structure and Strategic Positioning

### **8 MARKET ANALYSIS AND OPPORTUNITY ASSESSMENT**

#### 8.1 Market Drivers

#### 8.2 Market Restraints

#### 8.3 Net Impact of Drivers and Restraints

#### 8.4 SWOT Analysis: The PQC Market

#### 8.5 The Services-to-Product Ratio

- 8.6 Technology Readiness Assessment
- 8.7 The Opportunity-Assessment Framework
- 8.8 End-Use Market Opportunities
- 8.9 Per-Segment SWOT Analyses

## **9 INDUSTRY-SPECIFIC MIGRATION PROGRAMS**

- 9.1 Banking and Financial Services
- 9.2 Defence and Intelligence
- 9.3 Government and Public Sector
- 9.4 Telecommunications
- 9.5 Critical Infrastructure
- 9.6 Cloud and SaaS Providers
- 9.7 Healthcare
- 9.8 Automotive, IoT, and Manufacturing
- 9.9 Comparative Summary

## **10 MIGRATION SERVICES AND CONSULTING**

- 10.1 Market Structure
- 10.2 Pure-Play PQC Consultancies
- 10.3 Systems Integrators
- 10.4 Cloud-Vendor Migration Services
- 10.5 Specialty Hardware Vendors
- 10.6 Managed PQC Services and the Shift in the Services Mix
- 10.7 Strategic Implications for Service Providers

## **11 MARKET FORECASTS 2026–2036**

- 11.1 Total Addressable Market
- 11.2 Forecast by Cryptographic Approach
- 11.3 Forecast by Product Category
- 11.4 Forecast by End-User Group
- 11.5 Forecast by Region
- 11.6 Migration Services Forecast
- 11.7 Growth Scenarios

## **12 REGIONAL ANALYSIS**

- 12.1 North America
- 12.2 Europe
- 12.3 Asia-Pacific
- 12.4 Rest of World
- 12.5 Regional Forecast and Share Dynamics

## **13 COMPANY PROFILES (42 COMPANY PROFILES)**

## **14 RESEARCH METHODOLOGY**

- 14.1 Research Approach
- 14.2 Market Definition and Segmentation
- 14.3 Forecasting Model
- 14.4 Assumptions and Limitations

## **15 TERMS AND DEFINITIONS**

## **16 REFERENCES**

## List Of Tables

### LIST OF TABLES

- Table 1. PQC total addressable market — products vs. services 2026–2036 (millions USD)
- Table 2. Three types of cryptography relevant to the PQC transition
- Table 3. Reference Q-Day estimates by source, 2026
- Table 4. PQC algorithm families — characteristics and trade-offs
- Table 5. NIST-standardized post-quantum algorithms
- Table 6. PQC standards and standards bodies overview
- Table 7. Government and sector PQC migration mandates and deadlines
- Table 8. The quantum-safe migration stack — layers, function, and representative vendors
- Table 9. PQC market drivers — characterization
- Table 10. PQC market drivers and restraints
- Table 11. Driver and restraint impact scores
- Table 12. PQC market elements — Technology Readiness Level assessment, 2026
- Table 13. End-use opportunity ranking
- Table 14. Per-segment SWOT and recommended posture
- Table 15. Industry migration timelines and regulatory drivers
- Table 16. Estimated cumulative quantum-safe migration spend by sector (millions USD)
- Table 17. Quantum-safe migration services market by category, 2026–2036 (millions USD)
- Table 18. Total PQC addressable market 2026–2036 (millions USD)
- Table 19. PQC algorithm market by cryptographic approach 2026–2036 (millions USD)
- Table 20. PQC product market by category 2026–2036 (millions USD)
- Table 21. PQC product market by end-user group 2026–2036 (millions USD)
- Table 22. PQC product market by region 2026–2036 (millions USD)
- Table 23. Quantum-safe migration services market by category 2026–2036 (millions USD)
- Table 24. PQC algorithm & product market — growth scenarios (millions USD)
- Table 25. PQC product market by region 2026–2036 (millions USD)
- Table 26. Regional market characteristics summary

## List Of Figures

### LIST OF FIGURES

- Figure 1. Migration Services vs. PQC Products — the 8–12? Ratio (millions USD)
- Figure 2. Global PQC Total Addressable Market 2026–2036 (millions USD)
- Figure 3. PQC Algorithm & Product Market 2026–2036 (millions USD)
- Figure 4. PQC Market Drivers and Restraints
- Figure 5. Harvest-Now-Decrypt-Later: Why Migration Cannot Wait for Q-Day
- Figure 6. PQC Product Market by Region, 2036
- Figure 7. How a Quantum Computer Breaks Public-Key Cryptography
- Figure 8. Three Quantum-Era Security Approaches Compared
- Figure 9. PQC Market Map: Products, Services and End-Users
- Figure 10. Data Retention Windows vs. the Q-Day Risk Horizon
- Figure 11. Estimated Cumulative Probability of Q-Day, 2026–2046
- Figure 12. Indicative Quantum Hardware Roadmap vs. the CRQC Threshold
- Figure 13. The Four Families of Post-Quantum Cryptography
- Figure 14. PQC Algorithm Market Share by Approach 2026–2036 (% of value)
- Figure 15. Key and Signature Sizes: Classical vs. Post-Quantum (bytes, log scale)
- Figure 16. PQC Standardization and Migration-Mandate Timeline 2016–2036
- Figure 17. The Global PQC Regulatory Landscape
- Figure 18. The Quantum-Safe Migration Stack
- Figure 19. Crypto-Agility Maturity Model
- Figure 20. PQC Product Market by Category 2026–2036 (millions USD)
- Figure 21. PQC Product Categories: Margin vs. Market Size
- Figure 22. Net Impact of PQC Market Drivers and Restraints
- Figure 23. SWOT Analysis: The Post-Quantum Cryptography Market
- Figure 24. Technology Readiness of PQC Market Elements, 2026
- Figure 25. Technology Readiness vs. 2036 Market Size by Element
- Figure 26. Five-Step Framework for Exploring a PQC Market Opportunity
- Figure 27. End-Use Market Opportunity Matrix
- Figure 28. Industry Migration Timelines: Peak Activity Windows
- Figure 29. Cumulative Quantum-Safe Migration Spend by Sector (millions USD)
- Figure 30. Quantum-Safe Migration Services Market by Category 2026–2036 (millions USD)
- Figure 31. The Quantum-Safe Migration Services Provider Landscape
- Figure 32. Shift in Migration Services Mix, 2026 vs. 2036 (% of services market)
- Figure 33. Total PQC Addressable Market 2026–2036 (millions USD)
- Figure 34. PQC Algorithm Market by Cryptographic Approach (millions USD)

Figure 35. PQC Product Market by End-User Group, 2036 (millions USD)

Figure 36. PQC Product Market by Region 2026–2036 (millions USD)

Figure 37. PQC Algorithm & Product Market — Scenario Band (millions USD)

Figure 38. PQC Product Market Growth by Region 2026–2036 (millions USD)

Figure 39. Regional Share of PQC Product Market, 2026 vs. 2036

## I would like to order

Product name: The Global Post-Quantum Cryptography Market 2026–2036

Product link: <https://marketpublishers.com/r/G3728B901453EN.html>

Price: US\$ 1,400.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/G3728B901453EN.html>